République du SENEGAL

Un Peuple – Un But – une Foi

MINISTERE DE L'EDUCATION

DIRECTION DE L'ENSEIGNEMENT SUPERIEUR

INSTITUT AFRICAIN DE MANAGEMENT

7606 MERMOZ BP :15391
Dakar-Fann
Tél :338693636 Fax: 338277100
www.groupeiam.com

UMECUDEFS

118 Av André Peytavin Tél : 33 849 16 70 Fax : 33 842 33 87
BP 11545 DAKAR PONTY
www.umecudefs.com
contact@umecudefs.com

ETUDES ET MISE EN PLACE D'UN SYSTEME D'INTERCONNEXION DU RESEAU NATIONAL DE L'UMECUDEFS

Mémoire réalisé et soutenu par

Mr Youssef FEKRANE

Pour l'obtention du Diplôme d'Ingénieur Technologue en Informatique (DITI)

Email : youssef6dh@gmail.com Site web : www.youssefinfo.tk

Tél mobile: +221 77 510 05 06

Directeur de Mémoire

Mr Mamadou NIANG

Sous Directeur Production de la SDE

Professeur à l'IAM

Email :maniang@sde.sn Tél mobile :+221 77 642 04 45

Promotion : 2004/2008

Dédicaces

Louange à **Allah** le Tout Puissant et le Très Miséricordieux ;

Paix et salut sur tous ces prophètes particulièrement **Mohamed;**

Je dédie ce modeste travail ;

A mon oncle **Salah FEKRANE** pour son financement… ;

A mon père **Hammadi FEKRANE** pour son appui… ;

A ma chère mère **Fatna RACHOQUI** la femme exceptionnelle, pour son amour et sa tendresse… ;

A mes soeurs **Maryame, Fatima** et **mes frères Hamza** et **Abdou Allah ;**

A mes cousin **Anas, Zaid, Mouhamad, Tarik** et **Ayoub ;**

A toute la famille **FEKRANE** et **RACHOUQUI ;**

A mon encadreur **Mr Mamadou NIANG ;**

A tous les **professeurs** qui m'ont enseigné pour leur encouragements ;

A tous les **personnelles** de l'IAM ;

A tous les **personnelles** de l'UMECUDEFS ;

A **mes camarades** de promotion DITI 2008 ;

A tous ceux que je n'ai pas cités par oubli ;

A tous ceux qui m'aiment et m'ont soutenue ;

Que le bon Dieu prenne soin de vous comme vous avez pris

Soin de moi !

Remerciement

Nos remerciements vont particulièrement à l'endroit de M. **Mamadou NIANG,** pour son suivi et ses remarques avisées. Sa lecture minutieuse de ce document a beaucoup amélioré sa clarté. Puisse-t-il trouver ici l'expression de mon profond respect et de toute ma reconnaissance ;

Nos remerciements à tous nos professeurs de l'Institut Africain de Management, particulièrement à : M. **COLLINS**, M. **MBENGUE**, M. **TASSEMBEDO**, M. **A BA**,

M. **BAGUIDI**, Mr **K. DIOP**. Merci pour vos conseils, orientations et suggestions durant tout notre cursus ;

Merci à l'administration de l'**IAM**, pour la qualité d'enseignement qui nous a été donnée et qui a été pour nous un grand atout au cours de nos différents stages en entreprise;

Un clin d'œil particulier à **Mme NAFI FALL** chargée de la pédagogie de l'**IAM, Mme**

P. BAO ex directrice pédagogique, **Mr Moustapha Mamba Guirassy** Le président fondateur de l'IAM et **Mr Tijane SYLLA** Le directeur général de l'IAM ;

Nous tenons également à remercier Mme **MAGUI** qui, par son dynamisme, nous a trouvé le stage qui m'a ouvert les portes du monde professionnel;

A tout le personnel de l'UMECUDEFS pour leur disponibilité et sympathie ;

A **Mr Pape Ahmeth WADE** directeur de l'UMECUDEFS ;

A **Mr Meissa DIENG,** chef du service informatique ;

A Mlle **Laurence AMETEPE** pour son véritable soutient et affection ;

Aux frères de la vie : **Fabrice DOKO YOUBI, Abdou ellhay EL MARZOUQUI, Fadel SAKHO, Mouhamadou CISSE, Babcare SENE** et les non cités merci pour ses moments de bonheurs et de labeurs passés ensemble;

A tous les collègues de la promotion DITI 2008;

Sommaire

Liste des figures

Avant propos

Situé au quartier Mermoz Stéle à Dakar au Sénégal, l'Institut Africain de Management (I.A.M) a pour mission de former des cadres dans les domaines du management et de la technologie de l'information et de la communication.

Formation qui au bout de 4 ans, est sanctionnée par l'obtention d'un diplôme qui est une maîtrise, dénommée Bachelor In Business Administration (BBA) pour les manageurs et par le Diplôme d'Ingénieur Technologue en Informatique (DITI) pour les informaticiens.

Soumis à un certains nombres de critères pour l'entrée au sein de l'Institut, nous pouvons dire que l'entrée au premier cycle est réservée au titulaire d'un baccalauréat toute séries confondues, puis pour le second cycle il est réservé aux étudiants ayant déjà un BTS, DEUG ou autre diplôme équivalent.

Les spécialisations sont variées à l'I.A.M; notamment : la Finance, les Ressources Humaines, le Marketing, l'Audit Finance et la Communication des Entreprise sans oublier l'Informatique parallèlement à la formation initiale (cours du jour) l'I.A.M a su intégrer en son sein une formation continue qui s'adresse aux professionnels désireux de poursuivre leurs études (cours du soir). En 2003-2004 naissance d'un troisième cycle qui est sanctionné par un master.

Arrivé en quatrième (4ème) année, il nous est demandé de rédiger un mémoire de fin d'année marquant la fin de notre cursus. Ce mémoire devra faire l'objet d'une soutenance auprès d'un jury pour l'obtention de notre Diplôme.

Introduction

Les besoins en communication des entreprises ont fortement évolué notamment avec l'avènement des échanges électroniques au détriment du support papier.

La communication n'est pas seulement interne à l'entreprise mais aussi externe avec d'autres entreprises, des fournisseurs, des clients, des employés.

En effet, le nombre de travailleurs nomades et des agences est en augmentation et ces derniers peuvent avoir besoin d'accéder aux ressources de l'entreprise en tout lieu et à tout moment.

Pour répondre à ces besoins, de nouveaux moyens d'échange ont été développés à la base desquels on trouve l'informatique, les réseaux et Internet.

Aujourd'hui, de très nombreuses entreprises, quelle que soit leur taille ou leur activité sont connectées à Internet disposant ainsi, à travers ce réseau public, d'un point d'accès à une gigantesque infrastructure.

Mais l'utilisation d'Internet pose un problème de taille : la sécurité des échanges.

Cette sécurité est abordée sous plusieurs critères :

La disponibilité : les applications et services doivent être disponibles pour les utilisateurs.

L'intégrité : s'assurer que les données en transit ne peuvent être modifiées par une personne non autorisée sans que le destinataire ne s'en aperçoive.

La confidentialité : s'assurer que les données en transit ne peuvent pas être consultées par quelqu'un d'autre que le destinataire.

La preuve, non-répudiation : s'assurer qu'une entité à l'origine d'un message ou d'une transaction ne peut le nier à posteriori.

Toutefois, notre thème se base particulièrement sur l'étude et mise en place d'un système d'interconnexion du réseau national de l'UMECUDEFS qui permet de renforcer l'intégrité, la confidentialité et dans certains cas la preuve lors d'échange de données sur un réseau public.

Le travail que nous allons effectuer va s'étendre sur quatre grands axes bien distincts :

- Le cadre conceptuel, théorique et méthodologique dans lequel nous porterons une attention particulière de la problématique aux suggestions;
- Dans le deuxième axe, nous ferons les concepts généraux ;
- Dans le troisième axe, l'étude de l'existant ;

- Les préconisations techniques, organisationnelles et financières seront présentées dans le quatrième axe ainsi que l'étude de la mise en place du tel réseau de l'UMECUDEFS;

Partie I : Cadre conceptuel, théorique et méthodologique

Chapitre 1: Cadre conceptuel

1) Univers géographique, démographique et politique du pays

Le Sénégal se situe sur la pointe extrême occidentale du continent africain entre 12,5° et 16,5° de latitude nord et 12° et 17° de longitude ouest. C'est un pays qui couvre une superficie de 196 722 km^2. Le pays est bordé à l'ouest par 700 km de côtes sur l'océan Atlantique. Les Etats limitrophes du nord au sud sont : la Mauritanie, le Mali, la Guinée Conakry, la Guinée Bissau. Enclavée dans la partie sud, la Gambie a une ouverture sur l'océan. Le Sénégal est aligné sur l'heure du méridien de Greenwich (GMT). Les régions elles sont actuellement au nombre de 14, depuis la création de la région de Matam en 2001, puis celle de trois nouvelles régions en 2008 : Kaffrine au centre, Kédougou au sud-est et Sédhiou au sud, en Casamance, Dakar, Diourbel, Fatick, Kaolack, Kolda, Louga, Saint-Louis, Tambacounda, Thiès, Ziguinchor, Matam.

Dakar qui est la capitale administrative, fait aussi office de capital économique du Sénégal. Car elle regroupe la majeure partie des activités industrielles et commerciales (90%). Aujourd'hui le marché sénégalais s'élargie du fait de la compétitivité. Beaucoup des produit et des services sont présents sur le marché et représentent par la même occasion le domaine des micros finances.

2) Présentation de l'UMECUDEFS

2.1) Historique

L'UMECUDEFS est la dénomination de l'Union des Mutuelles d'Epargne et de Crédit de l'Unacois pour le Développement Economique et Financier du Senégal. Créée depuis 1997 à l'initiative de l'UNACOIS (Union Nationale des Commerçants et Industriels du Sénégal) suite au regroupement et à la fédération des caisses de base en novembre 2002 au sein d'une Union, UMECUDEFS. Le réseau dispose depuis le 22 mars 2000 d'un agrément officiel (n° DK 1 00 003U) délivré par le Ministère de l'Economie et des Finances en conformité avec la réglementation régissant les institutions de micro finance du Sénégal.

L'Union dispose d'une Direction Générale composée de différents services techniques destinés à coordonner et superviser les actions du réseau. Celui-ci est constitué en fin 2006

plus de 60 caisses créées de manière endogène et sur fonds propres par l'UNACOIS sur toute l'étendue du territoire national.

En effet, soucieuse, d'un développement économique et financier sans faille dans les zones les plus reculées du Sénégal, l'UMECUDEFS a décidé de mener une politique d'extension de son réseau dans le but de se rapprocher des populations où qu'elles se trouvent. C'est dans cette perspective que l'Union a implanté des mutuelles dans les quatorze régions du pays à savoir Dakar, Thiès, Kaolack, Fatick, Diourbel, Saint-Louis, Matam, Ziguinchor, Tambacounda, Louga, Kolda, Sédhiou, Kaffrine et Kédougou.

Les caisses sont localisées en majorité dans des centres commerciaux ou les marchés en référence au lien commun du réseau (sociétariat constitué majoritairement de commerçants, artisans et groupements féminins).

Actuellement le réseau dispose d'un potentiel important et fait partie des IMF les plus importantes du Sénégal grâce à une maîtrise de la croissance et à la qualité des produits et services.

2.2) Identité

Nom de l'institution : UMECUDEFS (Union des Mutuelles d'Epargne et de Crédit de l'Unacois pour le Développement Economique et Financier du Sénégal).

Figure 1.1.0 : *Logo de l'UMECUDEFS*

Sociétariat : Plus de 60.000 membres.

Nature de l'Institution : Institution de Micro finance.

Tél. : (+221) 33-849-16-70

Fax : (+221) 33-842-33-87

Site Web : www.umecudefs.com réalisé par M. Youssef FEKRANE, M. Fabrice DOKO YOUBI et M. KEBE

E-mail : contact@umecudefs.com

2.3) Localisation

La direction générale de l'UMECUDEFS est située au 118, avenue André Peytavin Dakar.

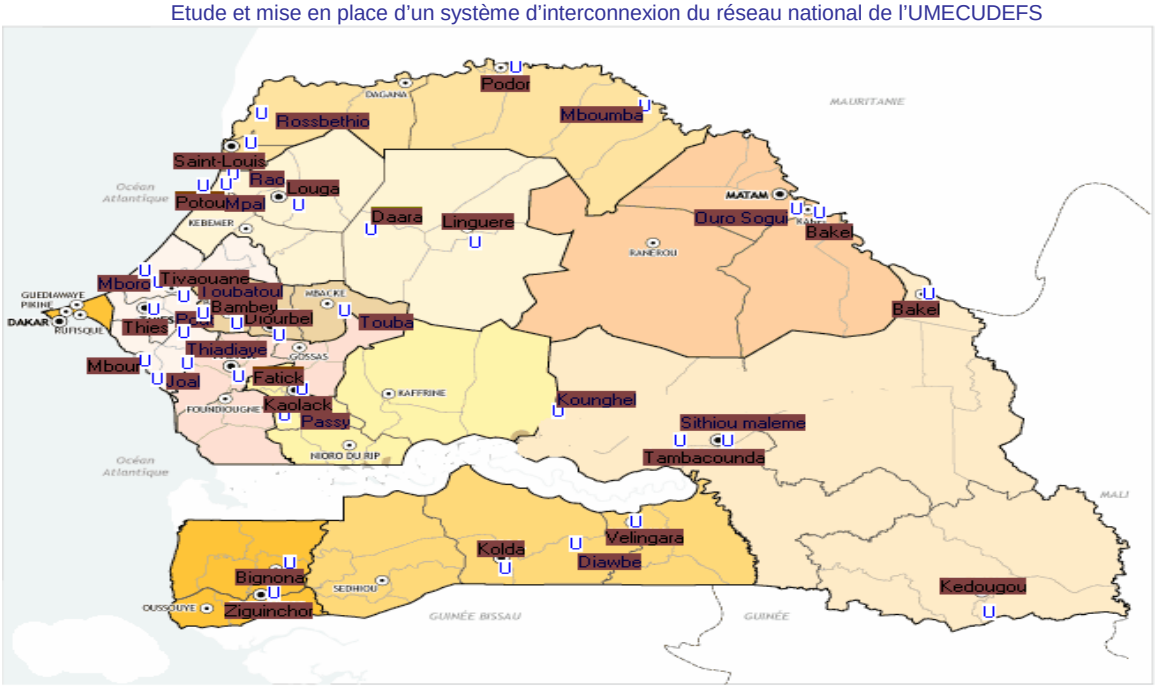


Figure 1.1.1 : Hors DAKAR 36 Mutuelles

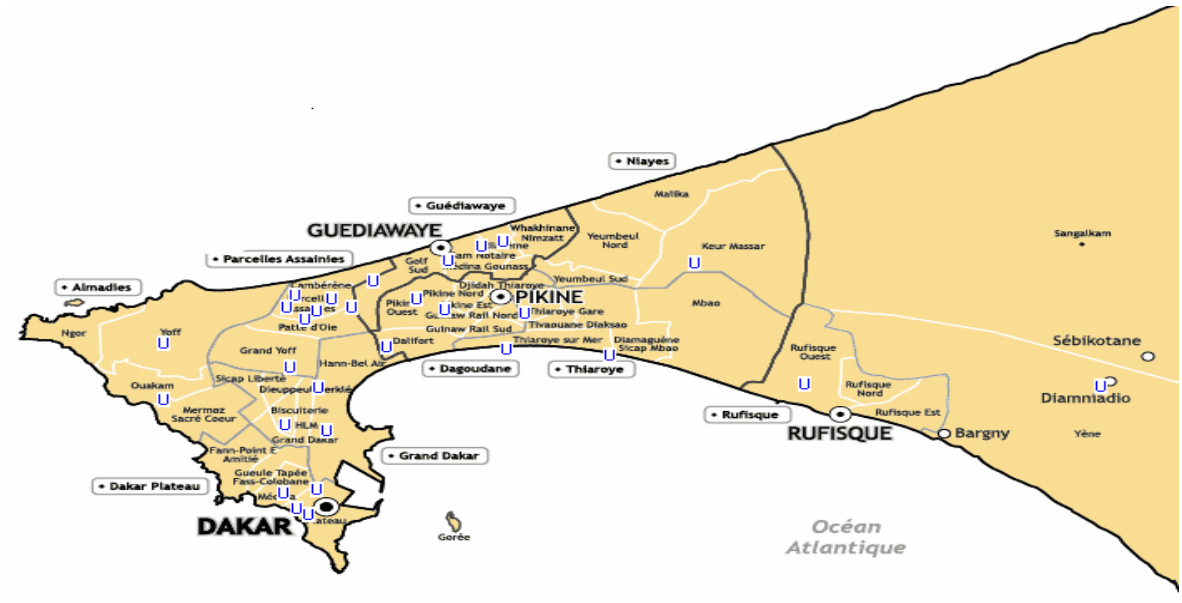


Figure 1.1.2 : Région de DAKAR 29 Mutuelles

2.4) Missions et objectifs

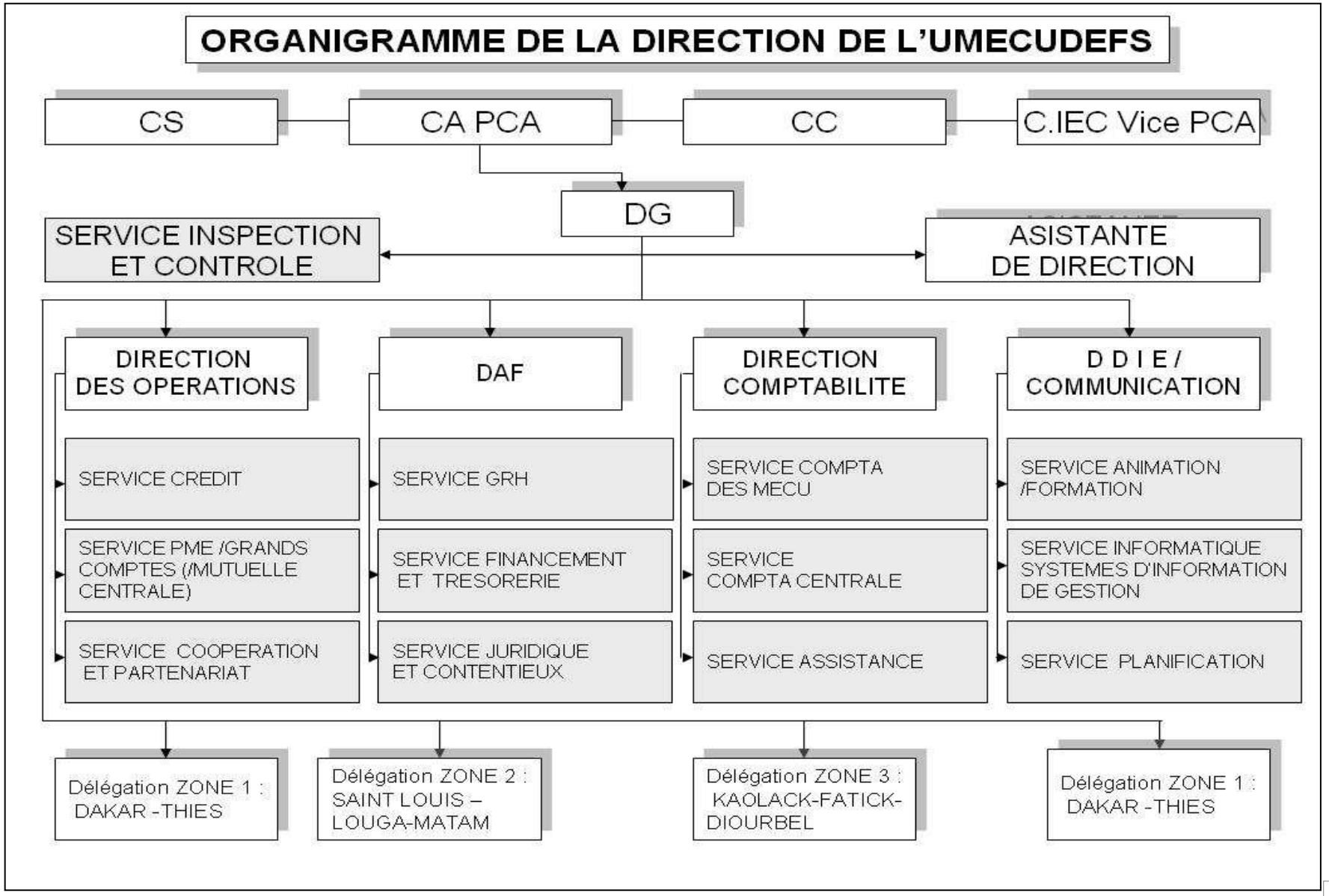
- Encourager l'esprit mutualiste au Sénégal;
- Faciliter l'accès au financement;
- Développer une culture d'entreprise chez les sociétaires;
- Sécuriser l'épargne des membres;
- Lutter contre la pauvreté.

- Collecter l'épargne de ses membres et leur consentir du crédit ;
- Promouvoir l'éducation économique, sociale et coopérative de ses membres ;
- Rechercher des financements (lignes de crédit, subventions…) ;
- Représenter collectivement les membres pour faire valoir leurs droits et intérêts communs ;
- Veiller au bon fonctionnement des membres ;
- Désigner les membres représentants de l'Union des Mutuelles d'Epargne et de Crédit pour le Développement Economique et Financier du Sénégal ;
- Prendre les initiatives nécessaires pour la création de nouvelles Institutions de base et de tous organismes jugés utiles au développement des Mutuelles d'Epargne et de Crédit pour le Développement Economique et Financier du Sénégal;
- Sanctionner, dans les cas de non respect par un ou plusieurs membres, par des textes ou politiques en vigueur ;
- Favoriser les activités commerciales, industrielles, agricoles et prestations de service ;
- Faciliter l'insertion des commerçants sénégalais dans les secteurs de l'industrie manufacturière notamment par la mobilisation des moyens de financement et le développement des ressources humaines ;
- Créer et développer un organe financier au sens de la Loi 95 -03 du 05 janvier 1995 ;
- La création ou la participation de toute entreprise, société ou groupement ayant un objet similaire ou connexe ;
- Et plus généralement la participation directe ou indirecte dans toutes opérations financières, commerciales et agricole ou industrielle pouvant se rattacher aux objets précités par voie de création de sociétés nouvelles, apport, souscriptions, achat de titres ou droits sociaux de fusion légalement admise, association ou autrement de nature à favoriser son extension ou son développement ;
- L'Union des Mutuelles d'Epargne et de Crédit pour le Développement Economique et Financier du Sénégal (UMECUDEFS), agit en outre en qualité d'organisme de surveillance et de contrôle de ses membres.
- Sous réserve des dispositions des précédents alinéas, l'UMECUDEFS est notamment chargée :

    - De fournir une assistance technique à ses membres en matière d'organisation, de fonctionnement, de formation et d'éducation,

- Exercer un contrôle administratif, technique et financier sur ses membres,
- Procéder, au moins deux fois par an, à l'inspection de ses membres,
- Assurer la cohérence et promouvoir le développement du réseau,

2.5) Organigramme de l'UMECUDEFS



CS : Conseil du Surveillance ;

CA : Conseil Administratif

PCA : Président Conseil d'Administration ;

CC : Comité du Crédit ;

C IEC : Comité Institut Etudes et Communication ;

DG : Directeur Général ;

Chapitre 2 : Cadre théorique.

1) Problématique

Les objectifs principaux d'une entreprise sont la réalisation de profits, la fidélisation des clients et faire face à la concurrence. Ces objectifs sont plus faciles à réaliser si l'entreprise suit l'évolution des technologies de télécommunication et l'accroissement important des services offerts.

Au Sénégal, les entreprises mettent en place plusieurs agences à travers Dakar et ses régions. Force de constater que beaucoup d'entreprises rencontrent des problèmes liés à l'indépendance de ces agences.

Dans le cas de l'UMECUDEFS, il a été constaté dans la gestion des mutuelles.

- Problème de communications entres les caisses de base et la direction.
- Problème des clients qui sont dépendant de la mutuelle où ils ont fait leur première adhésion.
- Des retards dans la transmission des données.
- Difficulté de l'intervention et la maintenance parfois demande un déplacement.

C'est à ce titre que l'UMECUDEFS a décidé de mettre en place un réseau visant à interconnecter l'ensemble de ses mutuelles.

Dans ce cas, Comment assurer la disponibilité, l'intégrité, la confidentialité et la fiabilité des données remontées par les mutuelles vers la direction ?

Nous allons subdiviser cette question on sous-questions.

- Quelle est la meilleure solution qui assure l'interconnexion et la sécurité du réseau de l'UMECUDEFS avec un coût raisonnable ?
- Comment on doit faire pour que la direction soit sur à l'abri contre les attaques ?

- Quel système mettre en place pour protéger et contrôler les hôtes du réseau ?
- Sur quelles bases se focaliser pour faire un choix pour une technologie propriétaire ou open source ?
- Quels seraient donc les bienfaits de la mise en place d'une telle technologie ?
- Comment intégrer cette solution au sein du système d'information de l'entreprise ?

2) Objectifs d'étude

2.1) Objectifs généraux

L'objectif principal de notre étude est de mettre en place un réseau sécurisé de l'ensemble des mutuelles (caisses de base) de l'UMECUDEFS. Notre travail va consister à étudier et à réaliser un système qui interconnecte toutes ses mutuelles dans le but d'améliorer la communication, de fidéliser nos clients et de sécuriser les informations relatives à ses principales activités.

2.2) Objectifs spécifiques

Les objectifs spécifiques sont :

- Appréhender les différents types des réseaux d'interconnexion existants pour mieux canaliser le choix pouvant répondre aux attentes de l'UMECUDEFS,
- Etudier les différents protocoles permettant la mise en place d'une solution,
- Choisir les techniques qui permettront d'optimiser l'utilisation de la solution choisie ;

3) Domaine de l'étude

Notre étude a été réalisée au Service Informatique et Système d'Information de gestion de la direction générale de l'UMECUDEFS.

4) Pertinence du sujet

La perspicacité de notre sujet peut être présentée à différents niveaux :

- **En entreprise** : notre travail serait un appui de décision dans les choix des processus de mise en place d'un réseau d'interconnexion qui permettrait d'assurer la communication entre les agences et le siége d'une quelconque entreprise ;
- **En milieu universitaire** : ce document pourra être un surplus de connaissances pour les futurs étudiants qui désireraient en savoir sur les différentes technologies d'interconnexion des réseaux existants ;

- **Dans l'administration réseau** : ce mémoire peut servir d'exemple dans les démarches de ceux qui aspireraient à étudier, analyser ou mettre en place un réseau similaire.

Chapitre 3 : Cadre méthodologique

1) Délimitation du sujet

Aujourd'hui l'informatique investit dans tous les domaines. Et tous les réseaux font émergences sans réserve. Demain, mêmes les plus petites entreprises devront disposer d'un réseau pour communiquer efficacement avec leur clientèle et leur environnement.

Mais la mise en place d'un réseau passe par différents critères techniques pour répondre aux attentes d'une entreprise. Ces critères influent sur le bon ou le mauvais fonctionnement du système de communication.

C'est la raison pour laquelle les instituts de micro finances notamment l'UMECUDEFS se sont vite intéressé à l'interconnexion des différentes agences.

Dans notre cas, le travail consistera à étudier et à réaliser un système d'interconnexion sécurisé entre les mutuelles et la direction générale de l'UMECUDEFS.

2) Technique d'investigation

Les méthodes et techniques d'investigations que nous avons utilisées au cours de notre étude sont :

- L'entretien direct avec les acteurs du système : ce procédé a permis d'avoir très rapidement des informations et de recenser les problèmes rencontrées ;
- L'observation des procédures et opérations ;
- La lecture des documents et la consultation de certains rapports de travail ont constitué un apport pour la réalisation de notre étude ;
- Nous avons aussi effectué des recherches sur des ouvrages traitant cette technologie, sur le web et bien sur les mémoires des anciens étudiants ;

3) Difficultés rencontrées

Durant notre étude, nous avons été confrontée à quelque difficultés telles que :

- certaines informations sont données par notre entreprise et exigeaient une confidentialité.
- Un léger retard dans le calendrier de démarrage du projet.

Partie II: Concepts généraux de l'étude

L'objectif de cette partie sera donc de faire le point sur les technologies et les solutions existantes en matière de connectivité inter-réseaux, les avantages et les inconvénients de chaque technologie.

Chapitre 1. Généralité sur les technologies des réseaux étendus.

Les réseaux étendus (ou WAN, Wide Area Network) se consacrent à l'échange d'informations sur de vastes aires géographiques. Ils sont, comme vous l'avez peut-être appris à propos de l'Internet, concernés par l'évolutivité - la capacité à s'accroître pour s'adapter au nombre d'utilisateurs du réseau et à répondre aux requêtes que ceux-ci adressent à ses ressources. Un réseau étendu - qui dépend de télécommunications pour couvrir de grandes distances - est généralement affecté d'un débit plus lent, de plus longs délais et d'un plus grand nombre d'erreurs qu'on en trouve généralement sur un réseau local. Mais il est aussi le moyen le plus rapide et le plus efficace aujourd'hui disponible pour transférer des données informatiques.

1) Les caractéristiques des réseaux étendus

Les réseaux étendus permettent à des utilisateurs distants (de différents endroits) d'accéder en temps réel à une base de données (un système transactionnel qui rassemble des données communes à plusieurs sites par exemple).

L'établissement d'un réseau étendu devra prendre en considération plusieurs facteurs :

1.1) Le support de communication :

- Le cuivre
- La fibre optique
- Les micro-ondes
- Les satellites
- La télévision par câbles

1.2) La vitesse de transmission

- Les lignes téléphoniques analogiques (RTC) qui permettent une connexion à un fournisseur d'accès à Internet :

  - Via un modem à 56 Kb/s
  - Via un modem ADSL
  - L'ATM en Large de Bande à 155 Mb/s

- Les lignes numériques :
- Les lignes à 56 Kb/s
- Les lignes IDSN (NUMERIS en France) à 128 Kb/s
- Les lignes T1 à 1,544 Mb/s (aux Etats-Unis)
- Les lignes E1 à 2,048 Mb/s (en Europe)
- Les lignes T3 à 45 Mb/s (aux Etats-Unis)
- Les lignes en fibres optiques des réseaux FDDI à 100 Mb/s
- L'ATM en Bande de Base à 622 Mb/s

1.3) Le mode de transmission

- La commutation de paquets (plusieurs chemins, les connexions sont dîtes « any-to-any ») :
  - Les lignes analogiques temporaires (RTC)
  - Le réseau analogique X25 en France
  - Le réseau numérique Frame Relay (Relais de Trames)
  - Les circuits virtuels (connexions logiques « point-to-many-point ») :
  - Les Circuits Virtuels Commutés (CVC ou SVC)
  - L'ATM
- Les circuits dédiés (un seul chemin, les connexions sont dîtes « point-to-point ») :
  - Les lignes analogiques louées, spécialisées
  - Les lignes numériques « point à point »

- Les circuits virtuels (connexions logiques « point-to-point ») :
- Les Circuits Virtuels Permanent (CVP ou PVC)
- Les réseaux privés Virtuels (RPV ou VPN)

1.4) Les protocoles réseaux

- Les protocoles d'accès à distance pour établir une connexion :
- SLIP (*Serial Line Internet Protocol*) ou CSLIP (Compressed Serial Link Internet Protocol)
- PPP (*Point to Point Protocol*)
- CHAP (Challenge Handshake Authentication Protocol)
- PAP (Password Authentication *Protocol*)
- BGP (Border Gateway *Protocol*) ou EGP (Exterior Gateway *Protocol*) pour les liaisons numériques

1.5) Les protocoles de transport

- TCP/IP

1.6) Les technologies ou architecteurs réseaux

- Relais de trames
- X.25
- ATM
- RNIS
- FDDI
- SONET
- SMDS

1.7) L'interconnexion des réseaux

- Des réseaux locaux (LAN)
- Des réseaux étendus (LAN, MAN & WAN) :

- Des réseaux privés
- Des réseaux publics :
- Via Internet
- Via un opérateur téléphonique

Les moyens nécessaires pour installer et maintenir des liaisons distantes sont tellement importants que les entreprises louent les services de **fournisseurs** internationaux.
Il peut arriver qu'un réseau utilise plusieurs types de supports de communication, plusieurs vitesse de transmission, plusieurs modes de transmission, plusieurs protocoles réseaux, plusieurs technologies ou architectures réseaux et plusieurs interconnections à plusieurs réseaux.

2) Les modes de transmission des réseaux étendus

Les modes de transmission des réseaux étendus peuvent se différencier soit par le type de signal (analogique ou numérique), soit par le chemin emprunté par les données (un chemin unique ou plusieurs chemins possibles). Les lignes peuvent être commutées (plusieurs chemins possibles) ou dédiées (un seul chemin) :

- La transmission analogique :
- Les lignes commutées du réseau RTC (plusieurs chemins)
- Les lignes louées (un seul chemin)
- La transmission numérique (les données transitent sur un circuit dédié, sauf pour le 56 commuté)
- La commutation de paquets (les paquets peuvent utiliser plusieurs chemins possibles)

Les Réseaux Privés Virtuels (RPV ou VPN) ne sont pas limités aux lignes téléphoniques spécialisées des liaisons numériques, mais ils peuvent aussi être mis en place via une ligne analogique et à travers le réseau Internet.

2.1) Le mode de transmission analogique

La transmission analogique s'effectue par l'intermédiaire des câbles des réseaux téléphoniques (Une paire de fils en cuivre) :

- Le Réseau Téléphonique Commuté (RTC) en France
- Le PSTN (Public Switched Telephone Network) en « anglais »

Les liaisons analogiques conviennent pour les connexions intermittentes de courte durée, elles ne sont pas aussi fiables que les autres modes de transmission, elles sont lentes et deviennent rapidement coûteuses. Les lignes analogiques ne proposent pas une qualité uniforme et régulière. Les lignes analogiques sont parfois perturbées par un bruit de fond qui induit un brouillage du signal. Les paquets de données doivent être retransmis et une partie de la bande passante non négligeable est utilisée pour la correction des erreurs.

La transmission analogique requière des modems de part et d'autre de la liaison. Les modems effectuent une conversion du signal, ce qui peut ralentir la communication. Les modems ont été inventés pour réduire le besoin des lignes numériques trop onéreuses. Les premiers modems transmettaient les données à 300 bits par secondes. Aujourd'hui, les modems transmettent à 56 Kb/s (en fait, la transmission est asymétrique, 53 Kb/s en **download** (réception) et seulement 33 Kb/s en **upload** (émission)). Une très grande partie des informations qui sont transmises par les modems serve au contrôle et à la correction des erreurs de transmission. Les modems se connectent au port série de l'ordinateur.

Les modems utilisent les ports séries des ordinateurs, et en général il n'y a que deux ports (COM1 et COM2) sur les ordinateurs INTEL. Toutefois, il existe des « cartes série multiport » qui se branchent sur la carte mère, et qui permettent de connecter plus de 16 modems différents sur la même carte série. Ainsi, il est possible de constituer ainsi un pool de modem qui augmente la bande passante disponible pour les utilisateurs d'un réseau LAN qui veut se connecter simultanément à Internet par exemple.

L'établissement d'une connexion avec un modem est un processus d'une trentaine de secondes.

Les fournisseurs de lignes téléphoniques proposent différents types de lignes :

- Les lignes commutées du réseau RTC sont les lignes téléphoniques standard. Les liaisons sur des lignes commutées sont temporaires avec plusieurs chemins possibles, elles sont ouvertes puis refermées, car la communication téléphonique longue distance reste

très cher. Les lignes commutées sont classées et numérotées de 1 à 10 en fonction de leur qualité. Les lignes de type 1 transmettent simplement la voix, tandis que les lignes de type 9 transmettent la voix et la vidéo par exemple…

- Les lignes louées sont des lignes téléphoniques spéciales ou spécialisées. Les lignes louées sont des liaisons permanentes et dédiées (un seul chemin). Les lignes louées sont plus rapides et plus fiables que les lignes commutées (plusieurs chemins).

Les fournisseurs de lignes proposent également des services ou des conditionnements qui accompagne la ligne proprement dite. Les conditionnements sont classés par des lettres (C ou D) et des chiffres (C1 à C8). Par exemple, une ligne 5/C3 est une ligne de type 5 avec un conditionnement C3…

❖ **Les lignes analogiques**

Les lignes analogiques du **réseau téléphonique commuté** (le RTC) permettent de communiquer à distance. Les lignes RTC ont l'avantage d'exister partout ou presque dans le monde, mais elles n'offrent pas la même qualité de service que les lignes numériques. Les communications distantes via une ligne analogique doivent passer par un modem pour transformer le signal digital des ordinateurs en une fréquence.

Les modems transmettent à des vitesses de 56 Kb/s et conviennent pour des liaisons de courte durée (avec un volume de données peu important comportant essentiellement du texte par exemple) et des liaisons peu fréquentes.

Les lignes DSL (Digital Subscriber Line) correspondent à une nouvelle technologie qui utilise les lignes analogiques (la paire torsadée en cuivre que l'on a tous chez soi), mais qui ne véhicule pas les données sous la forme de modulations de fréquences. L'inconvénient d'une ligne DSL est qu'elle est limitée à une longueur maximale de 6 Kilomètres, c'est à dire que la distance entre la prise de téléphone et le central téléphonique ne doit pas excéder 6 kilométres.

Il existe plusieurs technologies DSL :

- **L'ADSL** (Asymetric Digital Subscriber Line) convient pour l'accès à Internet parce que le flot de données entrantes (download) est plus rapide que le flot sortant (upload).

- **L'HDSL** (High-speed Digital Subscriber Line) transmet les données de façon symétrique (les vitesses sont les même dans les deux sens) mais sur une distance de 5 Kilomètres seulement. Les débits de l'HDSL sont voisins de ceux d'une ligne T1 (1,544 Mb/s).

- **Le RADSL** (Rate Adaptive Digital Subscriber Line) peut adapter la vitesse de transfert en fonction du support physique, mais reste limité à une distance maximale de 6 Kilomètres.

- **Le VDSL** (Very high bit-rate Digital Subscriber Line) ne dépassent 3 kilomètres pour une vitesse comparable à celle des LAN (10 Mb/s).

Le choix entre une ligne commutée ou une ligne louées dépend de plusieurs critères :

- La durée et la fréquence des communications
- Le coût
- Les débits
- La fiabilité
- Les types d'information véhiculés

2.2) le mode de transmission numérique

Le mode de transmission numérique est utilisé quand le mode de transmission analogique n'est pas à la hauteur des exigences du réseau (durée, débit,…). Les lignes numériques sont plus rapides et plus fiables que les lignes analogiques. Les lignes numériques sont utilisées pour transmettre n'importe quelles données (la voix, les données, les images, la vidéo,…). Le mode de transmission numérique n'a pas besoin de convertir les signaux avec des modems, puisque le signal reste numérique (dans l'ordinateur et sur le support de communication) ; pourtant, les transmissions numériques requièrent du matériel spécialisé. Le réseau est connecté à un pont ou un routeur, lequel est branché sur un CSU/DSU (Channel Service Unit / Data Service Unit), qui est lui-même relié à un répéteur, auquel est raccordée la ligne numérique. Le même dispositif se retrouve de l'autre coté de la liaison. Le CSU/DSU

convertit le signal numérique de l'ordinateur en un signal numérique bipolaire appartenant à l'univers des communications synchrones.

RESEAU + PONT + **CSU/DSU** + REPETEUR + **LIGNE** + REPETEUR + **CSU/DSU** + PONT + **RESEAU**

Les lignes numériques proposent des communications synchrones point à point. Les circuits "point à point" sont des circuits dédiés qui offrent une liaison permanente avec la garantie d'une bande passante bidirectionnelle simultanée (Full Duplex).

Il existe plusieurs modes de transmission pour les lignes numériques :

- **La commutation de paquets**
- **Le Frame Relay (ou Relais de trames)**
- **Les Réseaux Privés Virtuels (VPN)** qui utilisent le réseau Internet. Il est virtuel parce qu'il n'utilise pas de ligne spécialisée mais les supports de données d'Internet. Il est Privé parce que les données sont cryptées en utilisant un protocole de « tunneling ». Les VPN sont souvent basés sur des lignes numériques RNIS, mais ils peuvent également emprunter le réseau téléphonique analogique.

❖ **Les lignes numériques**

Les lignes numériques sont souvent appelées des lignes dédiées ou des lignes spécialisées. Elles sont obtenues auprès d'un opérateur téléphonique, et constituent généralement une liaison « point à point », c'est à dire un circuit réservé pour l'entreprise. Il existe plusieurs types de lignes numériques :

- **Les lignes DDS** (Digital Data Service) de 2 à 56 Kb/s.
- **Les lignes T1** n'existent qu'aux Etats-Unis.
  - Les lignes T1 offrent un débit de 1,544 Mb/s (la norme DS1).
  - Les lignes T1 sont appelées des lignes interurbaines parce qu'elles relient les grandes villes américaines depuis les années 1960.
  - Les lignes T1 peuvent être constituées de différents supports (du coaxial, de la fibre optique, des faisceaux hertziens,…)
  - Les lignes T1 utilisent le multiplexage (Multiplexing) inventé par BELL LABS (les réseaux téléphoniques commençaient à être saturés, une méthode, appelée « réseau T-Carrier », a permis de transmettre plusieurs appels en même temps

sur le même câble). Les signaux provenant de différentes sources convergent vers un multiplexeur qui les transmet au fur et à mesure. Les signaux sont ensuite démultiplexés et dispatchés.

  - Les lignes T1 sont très utilisées, mais très chers, aussi est-il possible de s'abonner à une ligne T1 partielle, c'est à dire à un ou plusieurs canaux de 64 Kb/s (la norme DS0). La bande passante d'une ligne T1 à 1,544 Mb/s est divisée en 24 canaux différents (Fractionnal T-1), chacun échantillonnés 8000 fois par seconde. Il est possible, selon ses besoins de s'abonner à un seul canal d'une ligne T1 ou éventuellement à plusieurs canaux, c'est l'agrégation de canaux, qui permet d'augmenter la vitesse d'une ligne numérique par incréments de 64 Kb/s.

- **Les lignes E1** correspondent aux lignes T1 en dehors des Etats-Unis, et offrent une vitesse de 2,048 Mb/s.
- **Les lignes T3** offrent les meilleures performances avec un débit de 45 Mb/s (la norme DS3 à un débit exacte de 44 736 Mb/s). Les lignes T3 requièrent un support à haute fréquence comme la fibre optique ou les micro ondes. Les lignes T3 sont utilisées par les très grandes entreprises et les fournisseurs d'accès à Internet. Les lignes T3 peuvent être utilisée dans leur totalité ou partiellement.
- **Les lignes 56 commutées** (Switched 56) sont la version commutée des lignes DDS. Les lignes 56 commutées peuvent être utilisées à la demande…

2.3) Le mode de transmission par commutation de paquets.

Le mode de transmission par commutation de paquets est utilisé pour transmettre des données sur de très longues distances. La commutation de paquets est fiable, rapide et commode. Les réseaux à commutation de paquets (Paquets-switching Networks) permettent de transférer des données en utilisant plusieurs chemins possibles (il n'y a pas de circuits dédiés). Les données sont fractionnées en petits paquets et chaque paquet est orienté sur la route optimale à un moment donné. Chaque paquet est commuté séparément. Les paquets qui arrivent à destination dans le désordre sont reconstitués. Le désassemblage et l'assemblage des paquets exigent un certain niveau d'intelligence.

Les réseaux à commutation de paquets sont constitués d'un maillage de plusieurs « échangeurs » qui lisent les paquets et les commutent. Afin d'optimiser le temps des « commutateurs » et de réduire la quantité des données retransmises (en cas d'erreur), la taille

des paquets est limitée. Les réseaux à commutation de paquets sont appelés des « connexions any-to-any ».

De nombreux réseaux à commutation de paquets utilisent des circuits virtuels (Virtual Circuits). Les circuits virtuels sont composés d'une série de connexions logiques (il ne s'agit pas d'une liaison physique dédiée entre les deux stations mais d'une bande passante allouée à la demande). Les réseaux virtuels à commutation de paquets sont appelés des « connexions point-to-many-point » :

- **Les Circuits Virtuels Commutés** (CVC ou SVC pour Switched Virtual Circuits) utilisent les ressources d'un réseau commuté pour établir une liaison dédiées, avec un seul chemin.
- **Les Circuits Virtuels Permanents** (CVP ou PVC pour Permanent Virtual Circuits) utilisent les ressources d'un réseau commuté pour établir une liaison dédiée et permanente qui ressemble à une ligne louée sauf que le client ne paye que la durée d'utilisation.

2.4) Le mode de transmission par commutation de label (MPLS).

MPLS (Multi-Protocol Label Switching) est une technique réseau en cours de normalisation à l'IETF dont le rôle principal est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 telles que implémentée dans ATM ou Frame Relay. MPLS doit permettre d'améliorer le rapport performance/prix des équipements de routage, d'améliorer l'efficacité du routage (en particulier pour les grands réseaux) et d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le coeur du réseau).

MPLS traite la commutation en mode connecté (basé sur les labels); les tables de commutation étant calculées à partir d'informations provenant des protocoles de routage IP ainsi que de protocoles de contrôle. MPLS peut être considéré comme une interface apportant à IP le mode connecté et qui utilise les services de niveau 2 (PPP, ATM, Ethernet, ATM, Frame Relay, SDH).

Objectifs et Missions du MPLS

L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des

gigarouteurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- Intégration IP/ATM
- Création de VPN
- Flexibilité : possibilité d'utiliser plusieurs types de media (ATM, FR, Ethernet, PPP, SDH).
- Differential Services (DiffServ)
- Routage multicast

La commutation de labels

Lorsqu'un paquet arrive dans un réseau MPLS (1). En fonction de la FEC auquelle appartient le paquet, l'ingress node consulte sa table de commutation (2) et affecte un label au paquet (3), et le transmet au LSR suivant (4).

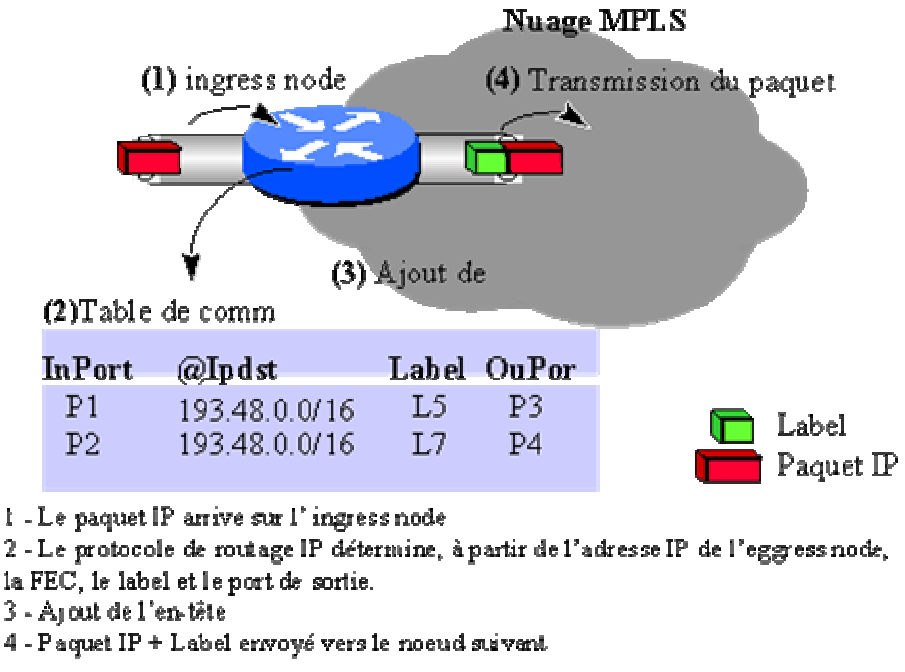


Figure 1.1.4 *: Label a l'entrer du réseau MPLS*

Lorsque le paquet MPLS arrive sur un LSR (1) interne du nuage MPLS, le protocole de routage fonctionnant sur cet équipement détermine dans la base de données des labels LIB

(Label Base Information), le prochain label à appliquer à ce paquet pour qu'il parvienne jusqu'à sa destination (2). L'équipement procède ensuite à une mise à jour de l'en-tête MPLS (swapping du label et mise à jour du champ TTL, du bit S) (3), avant de l'envoyer au noeud suivant (LSR ou l'egress node) (4). Il faut bien noter que sur un LSR interne, le protocole de routage de la couche réseau n'est jamais sollicité.

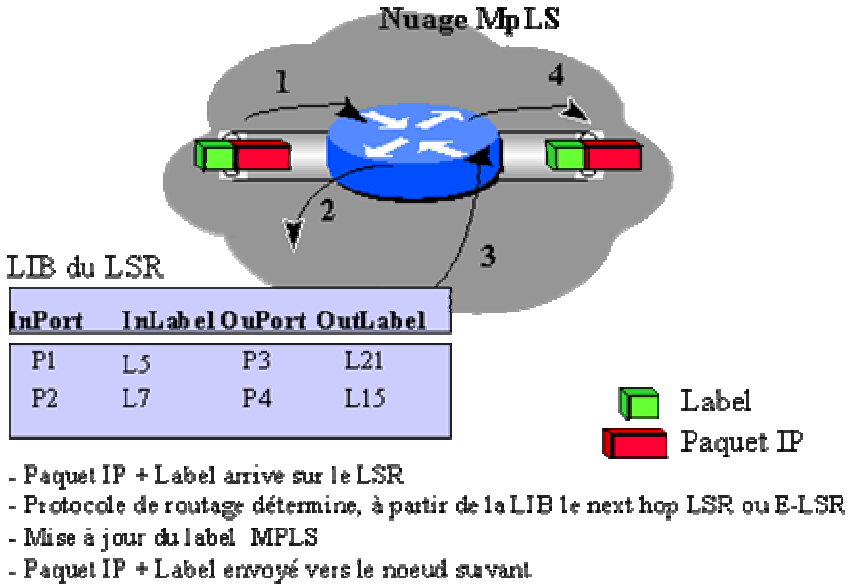


Figure 1.1.5 : *Label au niveau du LSR*

Enfin, une fois que le paquet MPLS arrive à l'egress node (1), l'équipement lui retire toute trace MPLS (2) et le transmet à la couche réseau.

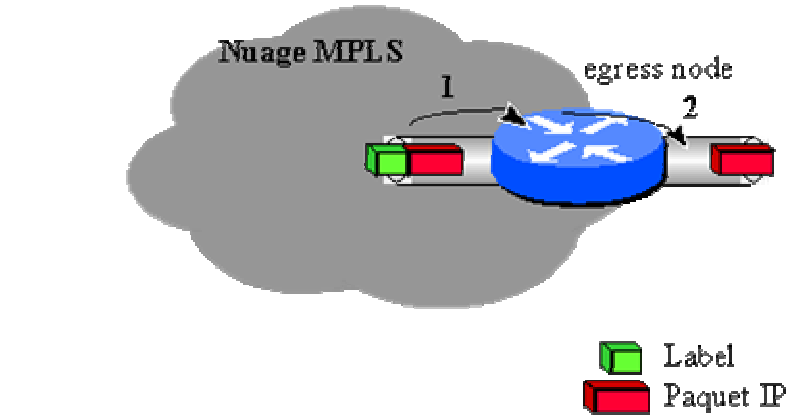


***Figure 1.1.6** : Label quitte le réseau MPLS*

- **Principes MPLS**

Basée sur la permutation d'étiquettes, un mécanisme de transfert simple offre des possibilités de nouveaux paradigmes de contrôle et de nouvelles applications. Au niveau d'un LSR (Label Switch Router) du nuage MPLS, la permutation d'étiquette est réalisée en analysant une étiquette entrante, qui est ensuite permutée avec l'étiquette sortante et finalement envoyée au saut suivant. Les étiquettes ne sont imposées sur les paquets qu'une seule fois en périphérie du réseau MPLS au niveau du Ingress E-LSR (Edge Label Switch Router) où un calcul est effectué sur le datagramme afin de lui affecter un label spécifique. Ce qui est important ici, est que ce calcul n'est effectué qu'une fois. La première fois que le datagramme d'un flux arrive à un Ingress E-LSR. Ce label est supprimé à l'autre extrémité par le Egress E-LSR. Donc le mécanisme est le suivant: Le Ingress LSR (E-LSR) reçoit les paquets IP, réalise une classification des paquets, y assigne un label et transmet les paquets labellisés au nuage MPLS. En se basant uniquement sur les labels, les LSR du nuage MPLS commutent les paquets labellisés jusqu'à l'Egress LSR qui supprime les labels et remet les paquets à leur destination finale.

L'affectation des étiquettes aux paquets dépend des groupes ou des classes de flux FEC (forwarding équivalence classes). Les paquets appartenant à une même classe FEC sont traités de la même manière. Le chemin établi par MPLS appelé LSP (Label Switched Path) est

emprunté par tous les datagrammes de ce flux. L'étiquette est ajoutée entre la couche 2 et l'entête de la couche 3 (dans un environnement de paquets) ou dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel dans les réseaux ATM). Le switch LSR du nuage MPLS lit simplement les étiquettes, applique les services appropriés et redirige les paquets en fonction des étiquettes. Ce schéma de consultation et de transfert MPLS offre la possibilité de contrôler explicitement le routage en fonction des adresses source et destination, facilitant ainsi l'introduction de nouveaux services IP. Un flux MPLS est vu comme un flux de niveau 2.5 appartenant niveau 2 et niveau 3 du modèle de l'OSI.

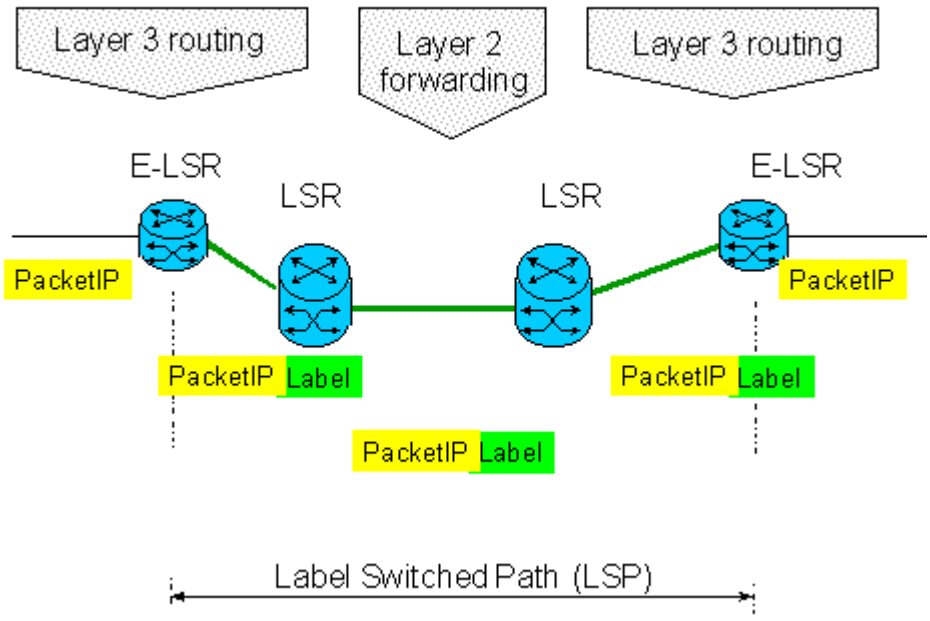


***Figure 1.1.7**: LSP (Label Switched Path)*

- **Label**

Un label a une signification locale entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et la LSR aval. A chaque bond le long du LSP, un label est utilisé pour chercher les informations de routage (next hop, lien de sortie, encapsulation, queueing et scheduling) et les actions à réaliser sur le label : insérer, changer ou retirer. La figure ci dessous, décrit la mise en oeuvre des labels dans les différentes technologies ATM, Frame Relay, PPP, Ethernet et HDLC. Pour les réseaux Ethernet, un champ appelé shim a été introduit entre la couche 2 et la couche 3. Sur 32 bits, il a une signification d'identificateur local d'une FEC. 20 bits

contiennent le label, un champ de 3 bits appelé Classe of Service (CoS) sert actuellement pour la QoS, un bit S pour indiquer s'il y a empilement de labels et un dernier champ, le TTL sur 8 bits (même signification que pour IP). L'empilement des labels permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversé du réseau MPLS.

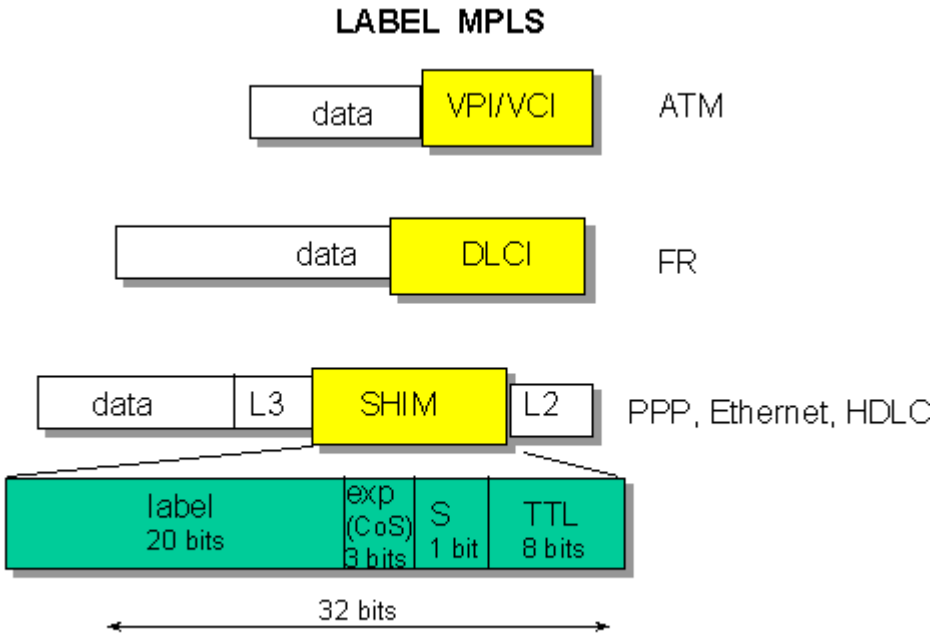


***Figure 1.1.8** : Mise en oeuvre de label MPLS*

3) Les technologies des réseaux étendus

Les réseaux étendus se présentent concrètement sous des dénominations qui englobent toutes les technologies qui permettent de réaliser une communication distante :

- **RTC**
- **Relais de trames**
- **X.25**
- **ATM**
- **RNIS**
- **FDDI**
- **SONET**
- **SMDS**

Les dispositifs de connectivité de chacune de ces technologie différent les uns des autres. Par exemple, un modem RNIS d'une ligne numérique « à la demande » n'est pas le même équipement qu'un commutateur CSU/DSU d'une ligne numérique « dédiée ».

3.1) les technologies à commutation du circuit :

3.1.1) Le Réseau Téléphonique Commuté (R.T.C):

Est le réseau du téléphone (fixe et mobile), dans lequel un poste d'abonner est relié à un central téléphonique par une paire de fils alimenté en batterie centrale (la boucle locale). Les centraux sont eux-mêmes reliés entre eux par des liens offrant un débit de 2 Mb/s : ce sont les Blocs Primaires Numériques (BPN).

Dans le cas d'un réseau construit par un opérateur public, on parle parfois de réseau téléphonique commuté public (RTCP).

Nous allons voir un certain nombre de caractéristiques (avantages, inconvénients) du RTC public utilisé pour le transfert de données numériques. Ce réseau qui est actuellement un des plus utilisés par les particuliers pour se relier entre eux ou à Internet.

Les avantages et les inconvénients du RTC pour ce type d'utilisation sont d'une part ceux inhérents au RTC lui-même, et d'autre part ceux induits par l'utilisation que l'on en fait, c'est à dire la transmission de données numériques.

Avantages

- **Commuté :** Il s'agit d'un réseau commuté, c'est à dire que lorsque la liaison est établie, on a l'impression d'avoir une ligne point à point. C'est très pratique pour la communication vocale ; ça évite d'avoir à recomposer le numéro du correspondant à fois que l'on veut prendre la parole.
- **Étendu** (géographiquement)**:** Le RTC public est très étendu ; il atteint tous les pays du globe, y compris les pays en voie de développement où même les villages très reculés possèdent en général au moins un téléphone.
- **Répandu** (nombre d'abonnés)**:** Beaucoup de personnes possèdent le téléphone. Si vous rencontrez une personne, vous lui demanderez sans doute son numéro de téléphone avant son adresse e-mail (à moins que vous n'ayez avec celle ci des relations de nature principalement informatique). Cette qualité est sans nul doute la principale, celle qui fait que l'on supporte tous les autres défauts inhérents à cette liaison. Elle a cependant un léger revers : malgré les efforts effectués pour élargir les lignes, un trop

grand nombre d'usagers simultanés peut provoquer des encombrements et empêcher l'établissement d'une communication.

- **Full Duplex :** Les deux utilisateurs de la liaison peuvent émettre et recevoir en même temps. Même si les hommes ne peuvent pas à priori parler et écouter en même temps (du moins, pas en comprenant ce qu'on leur dit), les modems sont parfaitement capables de réaliser cela et donc de tirer parti de la fonctionnalité full duplex du RTC.

Inconvénients

- **Analogique :** Le réseau téléphonique commuté est, normalement, analogique. Lorsqu'on l'utilise pour y transférer des données numériques, on connaît un certain nombre de restrictions :
  - **Nécessité d'utilisation de matériels spécifiques** pour faire la conversion analogique ↔ numérique. Ces appareils sont appelés *mod*ulateurs *dém*odulateurs, d'où le nom commun de « modem ».
  - **Limitation du débit**. En effet, d'une part, la bande passante (300-4000Hz) du RTC et d'autre part son rapport signal/bruit (de l'ordre de 40dB en moyenne) limitent la qualité du signal analogique transmis, ce qui se traduit par une limitation du nombre de bits que l'on peut faire passer par unité de temps. Les modems actuels arrivent à faire passer 33.6kb/s en full duplex. Pour dépasser cette limite, on a recours a des protocoles non symétriques comme le V90 (56kb/s en réception pour l'appelant seulement). Ces chiffres sont à comparer à ce qui est utilisé par FT pour numériser une liaison téléphonique : un échantillon de 8 bits (donnant un rapport signal/bruit maximum théorique de l'ordre des 54.2dB = 20xLog (0.5/2^8)) pris 8000 fois par secondes (nécessaire pour obtenir la bande passante à 4000Hz, théorème de Nyquist), soit un total de 64kb/s. Ce chiffre, qui est le débit d'un canal B d'une liaison RNIS, est le maximum qui puisse être réalisé sur un RTC sans compression. Ce débit maximal est en fait tout théorique, d'abord parce que le rapport signal bruit atteint rarement son maximum, et aussi à cause de l'occurrence de perturbations supplémentaires .D'où l'intérêt de passer à un RNIS comme Numéris pour bénéficier d'un débit maximal fixe et assuré de 64kb/s.
- **Perturbations :** Même une fois que la liaison du circuit virtuel est établie, un certain nombre de désagréments peuvent apparaître en cours de communication,

produisant des transmissions erronées et de ce fait limitant encore le débit, ou forçant purement et simplement un des modems à raccrocher.

- **Lignes physiques**. La plupart des lignes reliant les équipements de FT ne sont pas des liaisons radio, mais bel et bien des fils enterrés ou suspendus à des poteaux téléphoniques. Ceci implique qu'un coup de pelle mécanique malencontreux ou un accident renversant un de ces pylônes peut interrompre pour une durée élevée la liaison téléphonique.
- **Bruit**. Les équipements analogiques perturbent le signal transmis. Un transistor grillé ou une résistance ayant mal vieilli dans un équipement de FT ajoutent du bruit au signal lors de sa transmission.
- **Électromagnétisme**. L'orage ou un défaut d'antiparasitage sur un moteur passant dans les environs produit des crépitements sur la ligne, gênant les conversations et les modems !
- **Intermodulation**. Qui n'a pas déjà entendu une seconde conversation se surimposer à la sienne au téléphone ? Ceci peut avoir deux causes : soit les fils analogiques qui se longent sur une grande distance avant d'atteindre le central qui numérisera les conversations, soit lors du groupement/dégroupement des lignes.

o **Prix** : Le RTC est le relativement peu coûteux à mettre en place par rapport à une liaison spécialisé. Cependant, on n'achète pas la connexion au réseau, on la loue, ce qui peut à la longue s'avérer assez coûteux. Les liaisons courte distance ne sont pas très chères, et pour transmettre un message à un ami dans la même ville, il vaudra mieux lui passer un « coup de fil ». Pour des communications très longue distance comme pour transmettre des messages en Australie, l'utilisation d'un autre réseau comme Internet sera largement plus économique.

o **Sécurité** : Les lignes téléphoniques sont malheureusement assez accessibles aux personnes mal intentionnées, comme on le sait depuis l'affaire des écoutes téléphoniques. Étant commutées, elles sont cependant déjà plus confidentielles que les liaisons radio ou toute autre connexion de type bus, où chacun doit, de lui-même, se garder des messages qui ne lui sont pas destinés. Une solution à ces problèmes de sécurité est l'utilisation du *cryptage* sur la ligne téléphonique. Cette pratique est cependant restreinte en France et dans certains pays.

En résumé RTC avantages et inconvénients :

- ***AVANTAGES***
  - Disponibilité immédiate partout
  - Faible coût d'installation
  - On ne paye que le temps passé en ligne
- ***INCONVENIENTS***
  - Débit faible
  - Fiabilité de la communication sensible à la qualité de la ligne dans certaines conditions
  - Monopolise la ligne téléphonique

3.1.2) Réseau Numérique à Intégration de Services (RNIS) :

Le RNIS (Réseau Numérique à Intégration de Services), connu en France sous le nom commercial donné par France Télécom Numéris, est défini comme suit par le Livre Rouge de l'UIT-T : " Un réseau Numérique à Intégration de Services est un réseau développé en général à partir d'un réseau téléphonique numérisé, qui autorise une connectivité numérique de bout en bout assurant une large palette de services, vocaux ou non, auxquels les usagers ont accès par un ensemble limité d'interfaces polyvalentes ".

Le RNIS propose l'intégration des supports et des services. Pour cela, il s'appuie sur la numérisation et se développe au sein d'une structure puissante de normes internationales. Le RNIS, évolution du réseau téléphonique actuel, propose la continuité numérique de bout en bout. Il ne s'agit pas d'un réseau supplémentaire entrant en concurrence avec les réseaux existants comme le téléphone traditionnel, les réseaux X.25 ou les liaisons spécialisées. Le RNIS est plutôt un accès universel à ces réseaux, ou plus exactement à ces services supports. Cela implique donc une signalisation "intelligente" : la signalisation par canal sémaphore.

❖ **Les caractéristiques des réseaux étendus RNIS :**

- **Un réseau numérique à commutation de paquet**. Le réseau RNIS est la version numérique du réseau RTC.
- Un réseau RNIS (2B+D) à accès de base (Basic Access ISDN) permet de diviser la bande passante en trois canaux :
- **Deux canaux à 64 Kb/s appelés canaux B** qui peuvent être utilisés simultanément pour assurer un débit de 128 Kb/s.
- **Un canal à 16 Kb/s appelé canal D** pour la gestion des données et de la ligne

- **Un réseau RNIS à accès primaire** (Primary Access RNIS) utilise toute la bande passante d'une liaison T1 qu'elle peut diviser en 23 canaux B à 64 Kb/s et un canal D à 16 Kb/s.
- RNIS est une solution peu chère et adaptée pour les petites entreprises.
- **Les adaptateurs de terminaux IDSN** sont relié à l'ordinateur par l'intermédiaire d'un câble croisé (qui évite l'utilisation d'un concentrateur entre la carte réseau et l'adaptateur de terminal IDSN) qui se connecte au connecteur réseau (BNC, RJ 45, AUI,…) de la carte réseau Ethernet de l'ordinateur. C'est l'adaptateur de terminal IDSN qui compose le numéro de téléphone du réseau ISDN quand il reçoit des paquets de la part de l'ordinateur. Les adaptateurs de terminal IDSN conviennent pour le travail à domicile.
- **Le modem RNIS** est souvent un modem Bande de Base branché au port série d'un ordinateur. Les modems RNIS utilisent le protocole PPP pour établir la connexion.
- L'établissement d'une connexion RNIS est un processus de **2 ou 3 secondes**.

En résume RNIS avantages et les inconvénients

- ***AVANTAGES***
  - Débit supérieur à RTC
  - Délais de connexion inférieure à RTC
  - Disponibilité du téléphone
- ***INCONVENIENTS***
  - Pas de connexion permanente
  - Frais de mise en service assez élevés
  - Coût supérieur à RTC

3.2) Les technologies à commutation de paquets:

3.2.1) X25 :

Datant de 1970, X.25 est un protocole à commutation de paquets, orienté connexion ; il reposait à l'origine sur l'emploi de lignes téléphoniques analogiques et est resté pendant vingt ans le standard des communications en réseau. Les ordinateurs d'un réseau X.25 utilisent des communications full-duplex, qui démarrent lorsqu'un ordinateur en contacte un autre et que l'appelé répond en acceptant l'appel.

Bien que X.25 soit un protocole de commutation de paquets, son intérêt ne réside pas dans la façon dont ceux-ci sont routés de commutateur en commutateur entre réseaux, mais dans la définition des moyens par lesquels les ordinateurs expéditeur et destinataire (désignés par le sigle DTE) entrent en interface avec les dispositifs de communication (DCE) par lesquels passent de fait les transmissions. X.25 ne contrôle pas le chemin effectif emprunté par les paquets qui en constituent une ; aussi ce parcours représente-t-il une manière de nuée, comme l'indique l'illustration qui suit.

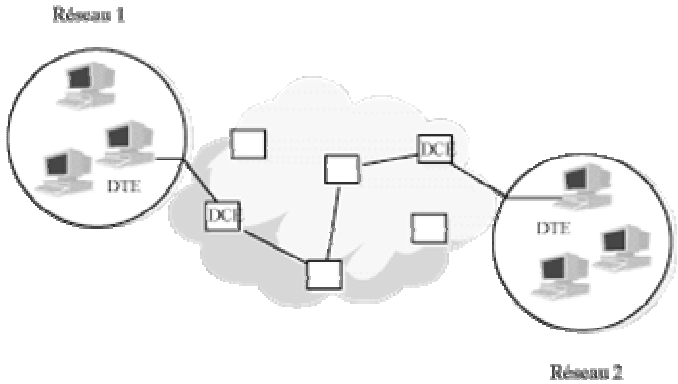


***Figure 1.1.9** : Fonctionnement du X25*

Une recommandation de l'ITU (anciennement le CCITT), X.25, se rapporte aux trois couches réseau les plus basses - Physique, Liaison et Réseau - du modèle de référence ISO :

3.2.1.1) Couche physique

- Au niveau de la couche la plus basse (Physique), X.25 spécifie les moyens - électriques, mécaniques, etc. - par lesquels la communication a lieu sur le support physique. À ce niveau, X.25 couvre des standards tels que RS-232, la spécification V.24 de l'ITU pour les connexions internationales et la recommandation V.35 de l'ITU pour les modems à grande vitesse transmettant des signaux sur plusieurs circuits téléphoniques.

3.2.1.2) Couche liaison

- Au niveau suivant (Liaison), X.25 couvre le protocole LAPB (Link Access Protocol, Balanced), qui définit les trames des paquets. LAPB garantit que deux dispositifs communicants peuvent établir une connexion exempte d'erreur.

3.2.1.3) Couche réseau

- Au niveau le plus élevé (en termes de X.25), la couche Réseau, le protocole X.25 couvre les formats des paquets, ainsi que le routage et le multiplexage des transmissions entre dispositifs communicants.

Sur un réseau X.25, les transmissions sont habituellement divisées en paquets de 128 octets. Elles peuvent comporter de 64 octets à un maximum de 4096 octets.

DTE et DCE. Comme cela a déjà été indiqué, les ordinateurs expéditeurs et destinataire sur un réseau X.25 ne sont pas appelés ordinateurs, hôtes, passerelles ou nœuds, mais DTE. Dans le langage X.25, ces DTE sont des périphériques transmettant les paquets aux DCE, suivant les liaisons qui constituent un réseau étendu. Les DTE se trouvent ainsi aux deux extrémités d'une connexion réseau ; les DCE résident pour leur part aux deux extrémités d'un circuit de communication, comme le montre l'illustration suivante.

***Figure 1.2.0**: Position de DTE et DCE*

PAD. Comme, cependant, les paquets sont aussi importants pour un réseau à commutation de paquets que les atomes le sont pour la matière, qu'en est-il des périphériques qui créent et ré-assemblent les paquets ? Dans certains cas, par exemple pour un ordinateur passerelle X.25 (le DTE) situé entre le réseau local et le réseau étendu, c'est lui qui va s'occuper de la mise en paquets. Dans d'autres cas, comme celui d'un PC ordinaire (autre type de DTE), le travail est géré par un dispositif appelé un PAD (Packet Assembler and Disassembler ou Assembleur/désassembleur de paquets). Dans ce cas, le PAD se trouve entre l'ordinateur et le réseau, plaçant les données en paquets avant de les transmettre ; lorsque tous ont été reçus, il reconstitue le message d'origine, en les replaçant dans le bon ordre.

Ce travail est-il difficile ? Pour un humain, sans doute, parce que les paquets sont envoyés par la meilleure route disponible au moment de leur transmission. Ainsi, il est tout à fait possible que des paquets représentant un seul message voyagent sur différentes liaisons et parviennent dans le désordre à destination. Vue l'importance du trafic sur un réseau étendu, et compte tenu du nombre possible de nœuds qui transmettent et reçoivent, le travail de reconstruction d'un

message quelconque représenterait donc une tâche herculéenne - mais le PAD n'en éprouve aucune difficulté.

❖ **Les caractéristiques des réseaux étendus X.25**

Le réseau X.25 est le réseau à Relais de Trames en France. Le protocole X.25 permet à des réseaux différents de pouvoir communiquer par l'intermédiaire de passerelles.

- **Un réseau analogique à commutation de paquets**. Le maillage est représenté sous la forme de nuages.
- Des fonctionnalités de **contrôle des erreurs très élaborées** mais qui consomment de la bande passante.
- **Une suite de protocoles X.25** qui définit l'interface entre les hôtes et les lignes louées (interface ETTD/ETCD) :
- Un hôte disposant d'une interface X.25
- Un PAD (Packet Assembler Disassembler)
- Une passerelle X.25
- Des nœuds de commutation

3.2.2) Frame Relay :

Le relais de trame est une nouvelle forme de la commutation de paquets, plus rapide et moins encombrante que X.25. On s'y réfère souvent comme à une technologique de commutation de paquets rapide ; le relais de trame transfère des paquets de longueur variable, jusqu'à 4 ko, et à des vitesses de 56 Kbps ou T1 (1,544 ou 3 Mbps) sur des circuits virtuels permanents.

Opérant uniquement au niveau de la couche Liaison, le relais de trame est plus rapide que le protocole X.25 car il supprime la majeure partie des informations de suivi, telles que la correction d'erreurs et le contrôle du flux du réseau, nécessaire dans un environnement X.25. Pourquoi ? Parce que le relais de trame, à la différence de X.25 qui dépendait à l'origine de connexions téléphoniques souvent peu fiables, a été conçu pour tirer parti des nouvelles possibilités de transmissions numériques, telles que les câbles en fibre optique et RNIS. Celles-ci sont fiables et pâtissent de peu d'erreurs, ce qui rend inutiles les types de mécanismes de vérification et de contrôle en usage sous X.25.

Si, par exemple, le relais de trame inclut bien un moyen de détecter des transmissions corrompues par un contrôle de redondance cyclique, ou CRC, lequel peut détecter si des bits

de la transmission ont changé entre source et destination, il n'en comporte pas qui corrige les erreurs. De façon analogue, comme il peut s'appuyer sur d'autres protocoles de couche supérieure pour garantir que l'expéditeur n'engorge pas trop rapidement le destinataire d'un trop grand nombre de données, il se contente d'inclure un moyen de répondre aux messages " trop de trafic en même temps" en provenance du réseau.

De plus, le relais de trame opérant sur des circuits virtuels permanents (PVC ou Permanent Virtual Circuit), les transmissions suivent un parcours connu et il n'est pas besoin de périphériques de transmission afin de déterminer la route préférable à tout moment donné. Elles n'ont pas vraiment de choix en la matière car les parcours utilisés dans le relais de trame sont basés sur des PVC appelés des DLCI (Data Link connexion Identifiers). Bien qu'un réseau à relais de trame puisse comporter un certain nombre de DLCI, chacun d'eux doit être associé de manière permanente à un trajet particulier pour une destination donnée.

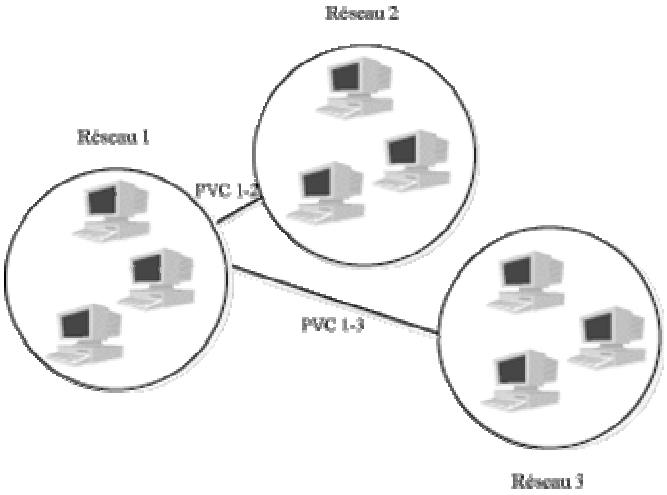


***Figure 1.2.1**: Fonctionnement du réseau relais de trame*

À ces questions de vitesse s'ajoute le fait que les périphériques d'un réseau à relais de trame n'ont pas à se préoccuper de reconstituer les paquets et/ou de rassembler les trames au fil de leur voyage. Par essence, le relais de trame fournit un service de bout en bout sur une route de communications numériques connue et rapide ; il s'appuie énormément sur la fiabilité offerte par les technologies numériques. En revanche, tout comme X.25, il est basé sur la transmission de paquets de longueur variable et définit l'interface entre les DTE et les DCE. Il s'appuie aussi sur le multiplexage d'un certain nombre de circuits (virtuels) sur une seule ligne de communication.

Comment le relais de trame fonctionne-t-il exactement ? À l'instar de X.25, les commutateurs de relais de trame dépendent d'informations d'adressage dans chaque en-tête de trame, pour déterminer où doivent être expédiés les paquets. Le réseau les transfère ensuite à une vitesse prédéterminée, dont il estime qu'elle permet un flux fluide d'informations durant les opérations normales.

Bien que les réseaux à relais de trame ne se chargent pas eux-mêmes de contrôler le flux des trames sur le réseau, ils s'appuient sur des bits spéciaux dans les en-têtes de trame, qui leur permettent de gérer l'engorgement du trafic. Leur première réponse face à ce problème consiste à envoyer une requête à l'application expéditrice, lui demandant de ralentir sa vitesse de transmission. La seconde se débarrasse des trames dotées d'un drapeau de livraison de priorité faible, réduisant ainsi de façon substantielle l'engorgement (on jette par-dessus bord une partie de la cargaison).

Les réseaux à relais de trame connectant des réseaux locaux à un réseau étendu dépendent, bien sûr, de routeurs et d'équipements de commutation capables de fournir des interfaces de relais de trame appropriées.

3.2.2.1) Couche physique

La couche physique utilise du bit stuffing (transparence binaire) : insertion d'un zéro tous les cinq 1 à l'émission et suppression du 0 suivant cinq 1 à la réception. Cette technique est pénalisante car elle introduit une irrégularité dans le débit utile. Elle est utilisée afin de s'assurer que la suite de bits 01111110 (0x7E, fanion des trames du Frame Relay) ne puisse apparaître « par hasard ».

L'interface physique n'est pas précisée par la norme, elle dépendra du constructeur ou de l'opérateur.

3.2.2.2) Couche liaison de données

La couche liaison de données est subdivisée en 2 sous-couches, le noyau (Core) et une sous-couche complémentaire et facultative non normalisée dont les fonctionnalités sont laissées à la discrétion des utilisateurs (EOP : Elément Of Procédure). Une utilisation typique est l'utilisation de la procédure HDLC LAPB comme sous-couche EOP. Cette sous-couche est utilisée uniquement par les équipements terminaux.

❖ **Les caractéristiques des réseaux étendus Relais de trames**

Les caractéristiques des réseaux étendus Relais de trames (Frame Relay) :

- **Un réseau numérique à commutation de paquets sur de la fibre optique** (fiable, rapide, sécurisé, et qui peut garantir une bande passante…) qui dérive des réseaux X.25 en France.
- Des fonctionnalités de contrôle des erreurs moins strictes que le X.25
- Des Circuits Virtuels Permanents (PVC) pour des « connexions point à point »
- Des trames de longueur variables
- Des commutateurs de données (Data Switch)
- Des ponts et des routeurs compatibles

Les réseaux étendus fonctionnant en Relais de Trames sont moins efficaces que les réseaux étendus fonctionnant sur des lignes numériques spécialisées. Il existe deux raisons qui expliquent ce phénomène :

- La vitesse de validation des information (le CIR pour Committed Information Rate) qui mesure la vitesse la moins bonne possible, c'est à dire la vitesse garantie. Le CIR est en général égal à la moitié de la bande passante annoncée.
- Le routeur chargé de transmettre les données doit empaqueter (ou encapsuler) les paquets du réseau local en un autre format, la « trame » qui est véhiculée sur le réseau étendu. Empaqueter les paquets et les dépaqueter prend du temps, ce qui affecte les performances des réseaux étendus en Relais de Trame.

L'alternative a cette inefficacité consiste à utiliser une « signalisation en bande de base » (CCS pour Clear Channel Signaling ou Common Channel Signaling). Avec le CCS, les données de signalisation utilisent un autre canal que les données proprement dites, et l'opérateur téléphonique n'a plus besoin d'empaqueter les données.

3.2.3) Réseau IP

Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

L'ambition d'Internet s'exprime en une phrase : relier entre eux tous les ordinateurs du monde. A l'image du téléphone qui permet de converser avec toute personne dont on connaît le numéro, Internet est un système mondial d'échange de documents électroniques : textes, fichiers, images, sons et séquences audiovisuelles.

C'est l'alliance de l'informatique et des télécommunications : la télématique au véritable sens du terme. Les utilisateurs d'Internet sont désignés par le terme d'internautes, synonyme de cybernaute, de surfer ou de net surfer. Quant aux informations du réseau, elles sont accessibles à partir de "lieux" que l'on appelle les sites Internet.

Ces quinze dernières années ont vu émerger de nouvelles techniques rendant possible l'interconnexion de réseaux différents (internet working) en les faisant apparaître comme un unique environnement de communication homogène. On désigne ce système d'interconnexion sous le nom d'internet, sachant que réseau Internet et Internet désignent l'ensemble de ces internets dont le point commun est de fonctionner en suivant les protocoles TCP/IP (Transmission Control Protocol/Internet Protocol). Le but de ce paragraphe est d'étudier comment fonctionne l'ensemble de ces protocoles

3.2.3.1) Architecture TCP/IP

L'architecture TCP/IP réside dans l'utilisation obligatoire du protocole IP, qui va avoir comme fonctions de base l'adressage et le routage des paquets IP. Le niveau IP correspond au niveau trois (3) du modèle OSI. Au dessus de IP deux protocoles ont été choisi : TCP et UDP, appartenant au quatre (4) intégrant une session élémentaire, ce qui fait que TCP et UDP prennent en chargent les fonctionnalités de niveau quatre (4) et cinq (5).

La différence provient d'un mode avec connexion pour TCP et sans connexion pour UDP. Le protocole TCP est très complet et permet de garantir une bonne qualité de service en particulier sur le taux d'erreur des paquets transportés. En revanche UDP est un protocole sans connexion qui supporte certaines applications moins contraignantes au niveau de la qualité de service. La couche qui se trouve au dessus de TCP-UDP regroupe des fonctionnalités de niveau six (6) et sept (7) de l'OSI et représente essentiellement le niveau application.

La pile de protocole TCP/IP est devenue le langage commun dans le monde des réseaux. Son usage est très répandu sur les réseaux d'entreprise. Elle constitue également le fondement du réseau mondial qui est internet, qui est en fait un gigantesque réseau de réseaux. Elle est aussi

le protocole de réseau par défaut de nombreux systèmes d'exploitation de réseau dont, Linux, Windows NT, 2003 serveurs.
La pile de protocole TCP/IP fait aujourd'hui partie intégrante des protocoles et composants logiciels qui permettent de faire fonctionner des routeurs d'un inter-réseau. Les administrateurs de routeurs Cisco utilisent Telnet (protocole membre de pile TCP/IP) pour communiquer avec les routeurs distants.

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle :

- **La couche physique** est l'interface avec le réseau, constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.
- **La couche Internet (réseau)** ou couche IP gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP et IGMP.
- **La couche transport** assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP ou non fiable dans le cas de UDP. Pour UDP, il n'est pas garanti qu'un paquet (appelé dans ce cas datagramme) arrive à bon port, c'est à la couche application de s'en assurer.
- **La couche application** est celle des programmes utilisateurs comme Telnet (connexion à un ordinateur distant), FTP, SMTP, etc.

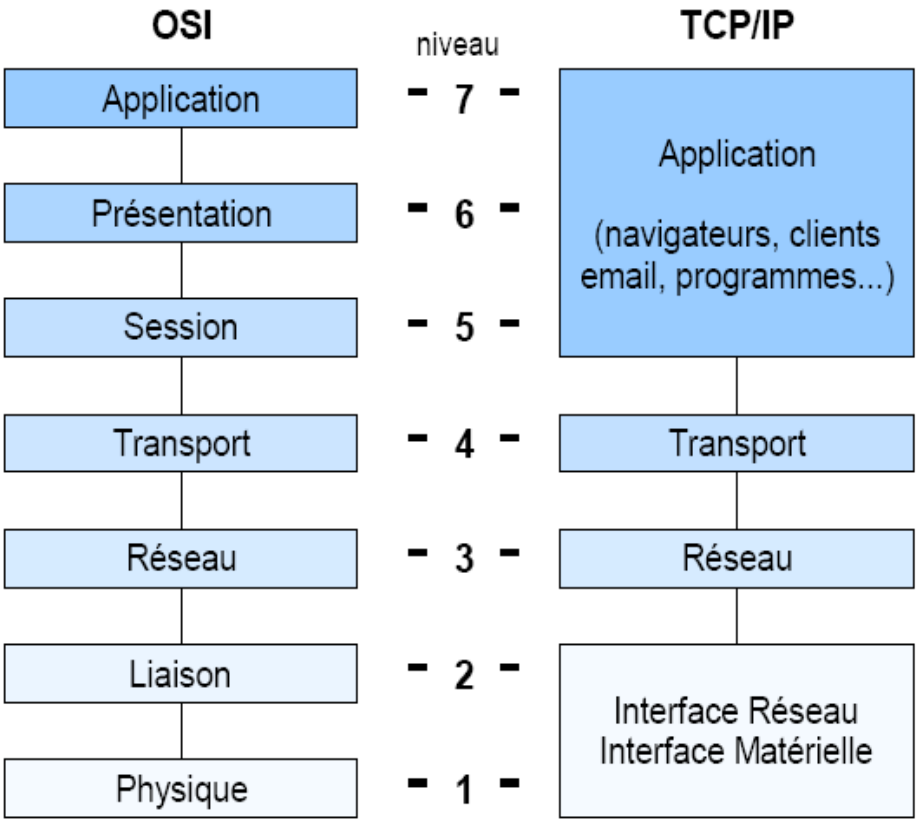


***Figure 1.2.2**: Les couches OSI et TCP/IP*

3.2.3.1.1) Couche application

Les protocoles qui interviennent au niveau de la couche d'application fournissent l'interface utilisateur destinée aux différents protocoles et aux différentes applications qui accèdent au réseau. Les protocoles de la pile TCP/IP qui interviennent au niveau de la couche application gérant le transfert des fichiers, les connexions distantes vers d'autres nœuds, les fonctions de courrier électronique et la surveillance du réseau. Différents protocoles interviennent à ce niveau :

- ***Telnet :*** C'est une application qui permet de se connecter à distance. Telnet définit une interface de communication, le terminal virtuel de réseau, pour que clients et serveurs n'aient pas à connaître les détails d'implantation de chaque système d'exploitation. De cette façon, les échanges se font dans un langage commun compris à la fois par le client et le serveur qui n'ont qu'à assurer une traduction de (ou vers) leur propre langage vers (depuis) ce langage cible.
- ***tftp et ftp :*** Ils permettent tous les deux de transférer des fichiers d'une machine à une autre. Cependant TFTP, bâti sur UDP, est beaucoup plus sommaire que FTP qui utilise

TCP. L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe. Donc, si l'utilisateur n'est pas reconnu la connexion FTP ne sera pas établie. Dans le cas particulier d'un serveur ftp public, la connexion se fait avec le nom anonyme et il est conseillé de donner son adresse électronique comme mot de passe. Dans le cas de TFTP, aucune authentification préalable n'est nécessaire. C'est pourquoi, lorsqu'un serveur TFTP est installé sur une machine il n'offre des possibilités d'accès qu'à un nombre restreint de fichiers bien spécifiques. Ces fichiers sont généralement des fichiers de démarrage de terminaux X ou stations sans disque.

- ***Smtp :*** Le courrier électronique au sein d'Internet est géré par le protocole SMTP bâti sur TCP (port 25). Il permet d'échanger des messages entre un expéditeur et un (ou plusieurs) destinataire pourvu que leurs adresses soient connues. Une adresse de courrier électronique se présente sous la forme nom@domaine est doit être composée de lettres (minuscules ou majuscules sont indifférenciées), de chiffres, de souligné (_) et de point (.). Il est à noter qu'un mécanisme d'alias permet de définir des équivalences entre adresses, notamment de préciser quelle machine parmi toutes celles d'un même domaine gère réellement le courrier de chaque utilisateur.

Une des caractéristiques principales du protocole SMTP est d'effectuer une remise différée du courrier qui assure que le service sera correctement rendu même si le réseau ou l'ordinateur destinataire sont momentanément en panne ou surchargée.

Un courrier expédié par un utilisateur est d'abord copié dans une mémoire de spool accompagné des noms de l'expéditeur, du récepteur, de l'ordinateur destinataire et de l'heure de dépôt. Puis le système de messagerie active en tâche de fond le processus de transfert de courrier qui devient un client. Il associe le nom de l'ordinateur destinataire à une adresse IP et tente d'établir une connexion TCP avec le serveur SMTP de celui-ci. Si cela réussit, le processus de transfert envoie une copie du message au destinataire qui l'enregistre dans une zone de spool spécifique.

Lorsque le client et le serveur se sont confirmés l'envoi et l'enregistrement complet du message le client supprime sa copie locale. Si le client n'arrive pas à établir une connexion TCP, ou si elle est rompue lors du transfert d'un message, il enregistre l'heure de cette tentative et réessaye quelque temps plus tard d'expédier le message. D'une manière générale un système de messagerie examine régulièrement sa zone de spool en envoi et tente d'expédier les messages (nouveau ou en attente à cause d'échec) qui s'y trouvent. Il finira par retourner à son expéditeur un message impossible à expédier après un délai

important. Ce mode de fonctionnement (établir une connexion de bout en bout) assure qu'aucun message ne peut se perdre, soit il est délivré, soit son expéditeur est prévenu de l'échec.

- ***Snmp :*** IL est le protocole d'échange des news 19 ou forums de discussions à travers Usenet (nom donné au réseau logique constitué des serveurs de news disséminés sur la planète). Il assure l'échange des news entre les serveurs et également la communication entre serveur et postes clients aussi bien pour la lecture que pour l'écriture de messages.
- ***Nfs :*** C'est un système qui permet de rendre transparente l'utilisation de fichiers répartis sur différentes machines. NFS utilise principalement UDP, mais ses nouvelles implantations utilisent également TCP. Lorsqu'un processus utilisateur a besoin de lire, écrire ou accéder à un fichier le système d'exploitation transmet la demande soit au système de fichier local, soit au client NFS. Dans ce dernier cas, le client NFS envoie des requêtes au serveur NFS de la machine distante. Ce serveur s'adresse à la routine locale d'accès aux fichiers qui lui retourne le résultat retransmis vers le client par la connexion UDP (ou TCP) IP. Il ne s'agit pas ici de transférer un fichier d'une machine à l'autre mais simplement de le rendre disponible de manière totalement transparente.

3.2.3.1.2) Couche transport

Les protocoles intervenant au niveau de cette couche offrent un contrôle de flux et garantissent la fiabilité de la connexion quand les données se déplacent d'un ordinateur émetteur vers un autre récepteur. Cette couche reçoit les données issues des protocoles de la couche application et commence à les préparer au déplacement en réseau. Deux protocoles cohabitent au niveau de cette couche : TCP et UDP

- ***Udp :*** Le protocole UDP utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui sont transmis par une application. UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues. Il ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis et il n'assure pas non plus de contrôle de flux. Il se peut donc que le récepteur ne soit pas apte à faire face au flux de datagrammes qui lui arrivent. C'est donc à l'application qui utilise UDP de gérer les problèmes de perte de messages, duplications, retards, déséquencement.

Cependant, UDP fournit un service supplémentaire par rapport à IP, il permet de distinguer plusieurs applications destinatrices sur la même machine par l'intermédiaire des ports. Un port est une destination abstraite sur une machine identifié par un numéro qui sert d'interface à l'application pour recevoir et émettre des données.

Le format détaillé d'un datagramme UDP est donné dans la figure ci-dessous. Les numéros de port (chacun sur 16 bits) identifient les processus émetteur et récepteur. Le champ longueur contient sur 2 octets la taille de l'en-tête et des données transmises. Puisqu'un datagramme UDP peut ne transmettre aucune donnée la valeur minimale de la longueur est 8. Le checksum est un total de contrôle qui est optionnel car il n'est pas indispensable lorsqu'UDP est utilisé sur un réseau très fiable.

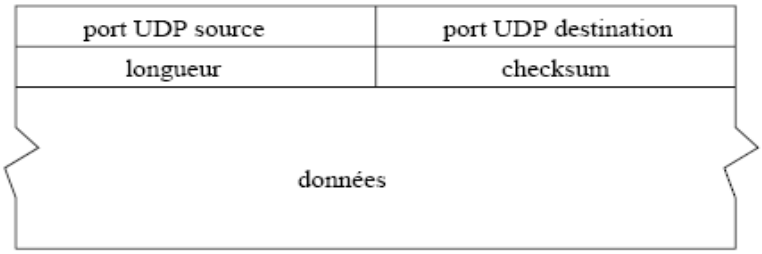


***Figure 1.2.3**: Structure d'un datagramme UDP*

- ***Tcp :*** Contrairement à UDP, TCP est un protocole qui procure un service de flux d'octets orienté connexion et fiable. Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à 6.

Le terme orienté connexion signifie que les applications dialoguant à travers TCP sont considérées l'une comme un serveur, l'autre comme un client, et qu'elles doivent établir une connexion avant de pouvoir dialoguer (comme dans le cas de l'utilisation du téléphone). Les ordinateurs vérifient donc préalablement que le transfert est autorisé, que les deux machines sont prêtes en s'échangeant des messages spécifiques. Une fois que tous les détails ont été précisés, les applications sont informées qu'une connexion a été établie et qu'elles peuvent commencer leurs échanges d'informations. Il y a donc exactement deux extrémités communiquant l'une avec l'autre sur une connexion TCP.

Cette connexion est bidirectionnelle simultanée (full duplex) et composée de deux flots de données indépendants et de sens contraire. Il est cependant possible d'inclure dans l'en-tête de segments TCP d'une communication de A vers B des informations relatives à la communication de B vers A. Cette technique de superposition (piggy backing) permet de réduire le trafic sur le réseau. La fiabilité fournie par TCP consiste à remettre des

datagrammes, sans perte, ni duplication, alors même qu'il utilise IP qui lui est un protocole de remise non fiable. Ceci est réalisé à l'aide de la technique générale de l'accusé de réception (ACK) présentée de manière simplifiée dans la figure ci-dessous.

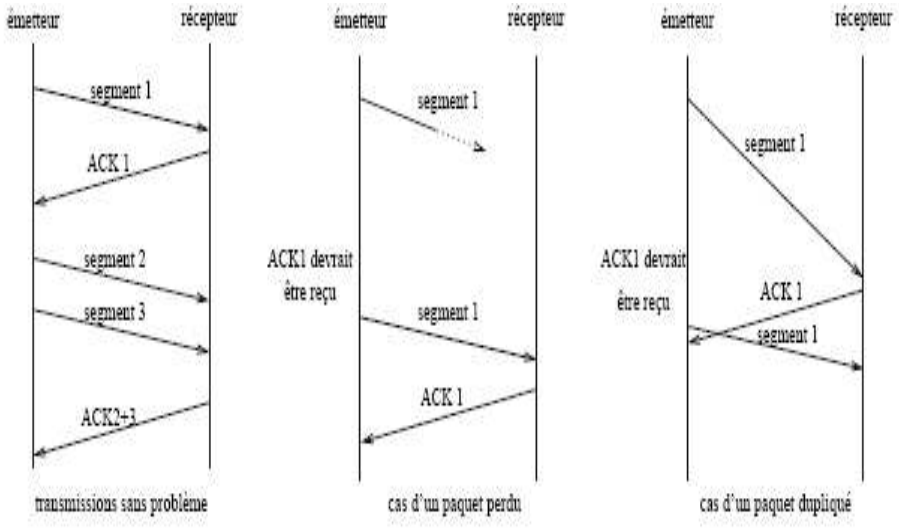


***Figure 1.2.4**: Échanges de segments TCP*

3.2.3.1.3) Couche Internet

La couche Internet correspond à la couche réseau du modèle OSI. Elle est responsable du routage des données au sein des chemins des réseaux logiques. Elle fournit aussi un système d'adressage aux couches supérieures. Elle définit également le format de paquet utilisé pour les données quand elles circulent au sein de l'inter-réseau. Cette couche repose essentiellement sur le protocole IP. Les autres protocoles qui interviennent au sein de cette couche gérant le système d'adressage IP et le format des paquets. Elle résout les adresses logiques (adresses IP par exemple) en adresses matérielles (MAC) correspondant au nœud du réseau. Différents protocoles interviennent à ce niveau :

- ***IP :*** Le protocole IP est au cœur du fonctionnement d'un internet. Il assure sans connexion un service non fiable de délivrance de datagrammes IP. Le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination. Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. On parle de remise au mieux (best effort delivery) et ni l'émetteur ni le récepteur ne sont informés directement par IP des problèmes rencontrés. Le mode de transmission est non connecté car. IP traite chaque datagramme indépendamment de ceux qui le précèdent et le suivent. Ainsi en théorie, au moins, deux datagrammes IP issus de la même machine et ayant la même destination peuvent ne pas suivre

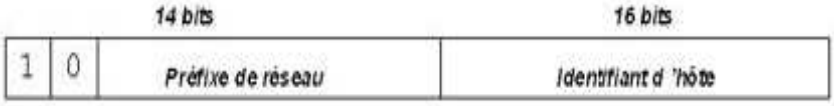
obligatoirement le même chemin. Le rôle du protocole IP est centré autour des trois fonctionnalités suivantes :

Premièrement définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet, deuxièmement définir le routage dans Internet et enfin définir la gestion de la remise non fiable des datagrammes

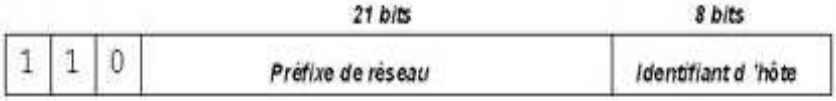
- **IPv4 :** Le protocole IPv4 se fonde sur un système de remise de paquets non fiable, que l'on appelle Best Effort (au mieux) et sans connexion. Le service offert et sans garantie car le paquet peut être perdu, dupliqué au remis hors séquence, sans qu'Internet ne le détecte ni n'en informe l'émetteurs, ni le récepteur. L'adressage IPv4 est représenté sur un entier de 32bits. L'adresse est constituée de deux parties : une partie identifiant le réseau et une autre identifiant la machine. Il existe quatre classes d'adresses permettant de coder un nombre différent de réseaux et de machine :

Classe A : 128 réseaux et 16 777 216 hôtes (7bits pour les réseaux et 24 pour les hôtes).

Classe B : 16 384 réseaux et 65 535 hôtes (16 bits pour les réseaux et 14 pour les hôtes).



Classe C : 2 097 152 réseaux et 256 hôtes (21bits pour les réseaux et 8 pour les hôtes).



Classe D : adresse de groupes (28 bits pour les hôtes).

- **IPv6 :** Enfin, le dernier moyen de contrer la pénurie progressive d'adresses est de changer de protocole réseau, de mettre en œuvre un nouveau protocole doté d'un champ d'adressage plus vaste. Cette solution radicale a pour avantage indéniable de résoudre une fois pour toute le problème, si tant est que le nouveau champ d'adressage soit suffisamment large pour durer indéfiniment

ou presque, et que la politique d'attribution des adresses soit contrôlée, afin d'éviter de gâcher inutilement de nouvelles adresses.

Le protocole IPv6 représente la nouvelle génération de protocole IP, d'où le nom de IPng (IP next génération). Il a été entièrement repensé. La nouvelle adresse sera sur 16 octets. La difficulté réside dans la représentation et l'utilisation rationnelle de ces 128 bits. La représentation s'effectue par groupe de 16 bits et se présente sous la forme suivante :

110 : FCBA : 1023 :AB32 :0 :0 : 34 : FEDC

Qu'une seule fois dans i' adresses égales à 0 peuvent êtres abrégées par le signe :: qui ne peut apparaître qu'une seule fois dans l'adresse. En effet ce signe n'indique pas le nombre 0 successifs ; pour le réduire, les autres séries ne peuvent pas être abrégées. L'adressage IPv6 constitue un adressage hiérarchique. Une allocation des adresses a été proposée.

- ***Arp/Rarp :*** Étant donné que le protocole IP, et ses adresses, peuvent être utilisés sur des architectures matérielles différentes (réseau Ethernet, Token-Ring, ...) possédant leur propres adresses physiques, il y'a nécessité d'établir les correspondances biunivoques entre adresses IP et adresses matérielles des ordinateurs d'un réseau. Ceci est l'objet des protocoles ARP et RARP. ARP fournit une correspondance dynamique entre une adresse IP connue et l'adresse matérielle lui correspondant, RARP faisant l'inverse.
- ***Icmp :*** Le protocole ICMP organise un échange d'information permettant aux routeurs d'envoyer des messages d'erreurs à d'autres ordinateurs ou routeurs. Bien qu'ICMP tourne au-dessus de IP il est requis dans tous les routeurs c'est pourquoi on le place dans la couche IP. Le but d'ICMP n'est pas de fiabiliser le protocole IP, mais de fournir à une autre couche IP, ou à une couche supérieure de protocole (TCP ou UDP), le compte-rendu d'une erreur détectée dans un routeur.

3.2.3.1.4) Couche d'accès réseau

Elle est constituée des protocoles qui prennent les datagrammes issues de la couche Internet, puis les enveloppent dans une trame de type spécifique, qui est ensuite placée sur le support du réseau physique sous forme d'un flux de bits. Comme ces protocoles résident au sein de la couche MAC (qui fait partie de la couche d'accès au réseau du modèle DOD et de la couche de liaisons de données du modèle OSI), ils sont impliqués intégralement dans l'adressage physique des paquets de données. Les interfaces de routeurs Ethernet et serial, Token Ring et

FDDI possèdent également des adresses MAC insolée dans la puce ROM du contrôleur de l'interface.

3.3) Les technologies à commutation de cellules ATM :

ATM, on le sait, est le sigle de Asynchronous Transfer Mode (Mode de transfert asynchrone). Mais qu'est-ce exactement, et quels avantages offre-t-il ?

Il s'agit d'une méthode de transport capable de livrer, non seulement des données, mais aussi de la voix et de la vidéo, simultanément et sur les mêmes lignes de télécommunication. Généralement considérée comme la nouvelle génération de transport, en termes d'accroissement des capacités des réseaux locaux et des réseaux étendus, ATM est une technologie réseau orientée connexion, étroitement liée à la recommandation de l'ITU pour RNIS à large bande (BISDN ou broadband ISDN) révisée en 1988. ATM se révèle particulièrement intéressante pour la communication réseau à grande vitesse des réseaux locaux et des réseaux étendus, sur une gamme de supports allant du câble coaxial traditionnel au câble en paire torsadée et aux fibres optiques, pour les services de communication du futur telles que Fibre Channel, FDDI et SONET.

Relais de cellules. ATM, tout comme X.25 et le relais de trame, se fonde sur la commutation de paquets. À leur différence toutefois, il recourt au relais de cellules, méthode de transmission à grande vitesse basée sur des unités de taille fixe (petites unités de longueur limitée à 53 octets), appelées des cellules, qui sont multiplexées sur la porteuse.

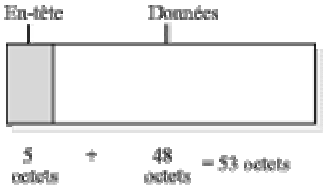


Figure 1.2.5 *: Une cellule*

Le fait que des cellules de taille uniforme voyagent plus vite et puissent être routées plus rapidement que des paquets de longueur variable est une raison - il en est d'autres - expliquant la rapidité d'ATM. La transmission s'effectue généralement à une vitesse de 1,544 Mbps, mais l'ITU a aussi défini des vitesses d'ATM jusqu'à 622 Mbps (sur câble en fibre optique).

Fonctionnement. Imaginez une machine universelle - capable d'accepter tous types de matériaux, qu'ils soient livrés sporadiquement ou selon un flux constant, et qui les transforme en paquets identiques. C'est fondamentalement la manière de fonctionner d'ATM. Il accepte des flux de données (voix, vidéo, peu importe) et les conditionne sous forme de cellules uniformes de 53 octets. En sortie, il les envoie sur le réseau étendu afin de constituer un flux continu jusqu'au lieu de livraison, comme l'indique la figure 1.2.6.

Tout semble suffisamment simple, mais examinons de plus près l'intérêt effectif d'ATM.

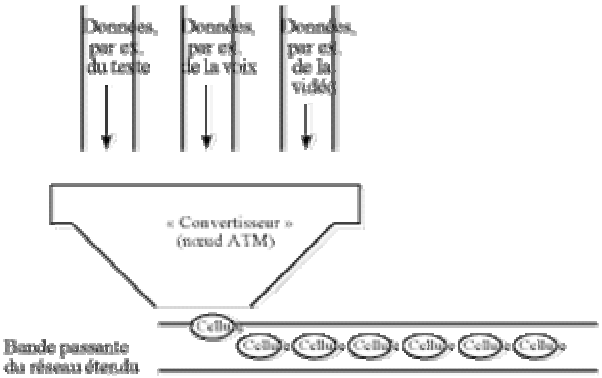


Figure 1.2.6*:ATM brise les flux de données en cellules de taille fixe et les livres sur un réseau étendu.*

Le convertisseur, ici, n'est pas un véritable commutateur ATM - il rappelle une trémie ou un entonnoir, à travers lequel s'écoulent les différents flux de données. La représentation est approximative, mais conceptuellement exacte.

Pour commencer, rappelez-vous qu'ATM est conçu pour permettre la livraison de flux multimédias, lesquels recouvrent des types différents d'informations aux caractéristiques également différentes, que gèrent aussi différemment les périphériques qui les traitent aussi bien que les protocoles réseau de plus haut niveau. Toutefois, pour utiliser ATM, il doit exister un élément qui forme interface avec ces différents dispositifs, pour empaqueter ces types de données afin de les transporter. Cet élément est le nœud ATM, qui gère les conversions spécifiées dans le modèle à trois couches d'ATM, que donne l'illustration suivante.

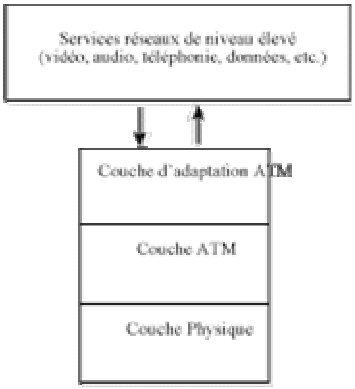


***Figure 1.2.7** : Trois couches d'ATM*

Voici ce que font ces couches :

3.3.1) **La couche supérieure, AAL** (ATM Adaptation Layer ou Couche d'adaptation ATM) se trouve entre ce que l'on peut considérer comme l'ATM véritable et les périphériques et protocoles réseau de niveau supérieur, qui envoient et reçoivent les différents types d'informations sur le réseau ATM. AAL, comme le mot adaptation le suggère, sert de médiateur entre la couche ATM et ces protocoles de niveau supérieur, en remodelant les services de l'un pour qu'ils s'adaptent aux services de l'autre. Cette disposition est assez fascinante, dans la mesure où AAL récupère les différentes formes de données (audio, vidéo, trames de données) et les transmet à des services AAL comparables (audio, vidéo, trames de données) qui les conditionnent en unités de 48 octets, avant de les passer à la couche ATM où elles subissent un traitement supplémentaire.

3.3.2) **La couche ATM** attache des en-têtes aux unités ATM. Cela peut sembler simple, mais cet en-tête ne dit pas simplement " ceci est une cellule". Il comporte entre autres des informations identifiant les chemins et circuits sur lesquels voyageront ces cellules, ce qui permet aux commutateurs et routeurs ATM de les livrer correctement aux destinations prévues. La couche ATM multiplexe aussi les cellules pour la transmission, avant de les passer à la couche physique. Celle-ci, comme vous le voyez, a beaucoup de travail à effectuer.

3.3.3) **La couche physique**, la plus basse, correspond à la couche Physique du modèle de référence ISO/OSI. Comme dans le modèle OSI, elle s'occupe du déplacement des informations - dans le cas présent, des cellules ATM de 53 octets - sur le support de communication. Comme nous l'avons déjà indiqué, ce support peut

être varié : fibres optiques basées sur SONET (Synchronous Optical NETwork), lignes T1 ou E1, voire modem. Le médium et le message, dans ce cas, sont clairement séparables, car ATM est une méthode de transport, indépendante des supports de transmission sur lesquels voyagent les messages.

Que se passe-t-il après qu'ATM a filtré les informations jusqu'aux couches AAL, ATM et Physique ? Une fois que la couche physique a envoyé les cellules, celles-ci voyagent jusqu'à leur destination sur des connexions qui peuvent les commuter d'un circuit à un autre. En chemin, les commutateurs et routeurs font en sorte de conserver des connexions offrant au réseau le minimum de bande passante au moins nécessaire pour donner aux utilisateurs la qualité de service (QOS ou quality of services) qui leur est garantie.

Lorsque les cellules arrivent à destination, elles subissent le processus inverse de celui de l'expédition. La couche ATM transmet les cellules aux services appropriés (voix, données, vidéo) de l'AAL, où leur contenu est reconverti sous sa forme originelle ; tout en est vérifié, pour garantir que la livraison est sans erreur, et les informations reconstituées sont passées au dispositif récepteur.

Disponibilité. ATM est donc un merveilleux moyen de transmettre toutes sortes d'informations à grande vitesse. Il est fiable, flexible, évolutif et rapide, parce qu'il dépend des protocoles de plus haut niveau pour le contrôle d'erreurs et leur correction. Il peut entrer en interface avec les réseaux à large bande et à bande étroite, et il convient particulièrement à une dorsale de réseau.

Comporte-t-il des inconvénients? Oui, bien sûr. Tout d'abord, les réseaux ATM doivent être constitués de périphériques compatibles ATM, onéreux et peu répandus. De plus, leur déploiement pose un problème sérieux : les entreprises ne sont pas prêtes à s'engager dans des dépenses d'investissements en équipements ATM, si les services ATM ne sont pas facilement disponibles à grande échelle dans les entreprises de télécommunications ; ces dernières sont peu disposées à investir dans des solutions de communications réseau ATM si la demande est trop faible.

3.4) Les technologies numériques dédiés :

xDSL :(DSL pour Digital Subscriber Line et x pour désigner une famille de technologies) - Nouvelle technologie WAN en développement pour un usage domestique. Offre une bande

passante qui diminue en fonction de la distance par rapport à l'équipement de l'opérateur. Des vitesses maximales de 51,84 Mbits/s sont possibles à proximité d'un central téléphonique, mais des débits largement inférieurs sont plus courants (de quelques centaines de Kbits/s à plusieurs Mbits/s). D'un usage peu répandu, mais en augmentation rapide, son coût est modéré et en baisse. Le caractère x indique l'ensemble de la famille de technologies DSL, dont :

- HDSL - Ligne numérique (DSL) à haut débit binaire
- SDSL - Ligne numérique (DSL) à débit symétrique
- ADSL - Ligne numérique à paire asymétrique (DSL asymétrique)
- VDSL - Ligne numérique asymétrique (DSL) à très haut débit
- RADSL - Ligne numérique (DSL) à débit adaptable

Chapitre 2. La sécurité informatique :

1) Principes de la sécurité

1.1) Exigences fondamentales

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

1.1.1) Disponibilité : demande que l'information sur le système soit disponible aux personnes autorisées.

1.1.2) Confidentialité : demande que l'information sur le système ne puisse être lue que par les personnes autorisées.

1.1.3) Intégrité : demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

La sécurité recouvre ainsi plusieurs aspects :

- Intégrité des informations (pas de modification ni destruction)
- Confidentialité (pas de divulgation à des tiers non autorisés)
- Authentification des interlocuteurs (signature)
- Respect de la vie privée (informatique et liberté).

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Cette menace peut-être accidentelle, intentionnelle (attaque), active ou passive.

1.2) Étude des risques

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé.

Il faut cependant prendre conscience que les principaux risques restent : « câble arraché », « coupure secteur », « crash disque », « mauvais profil utilisateur ».

Voici quelques éléments pouvant servir de base à une étude de risque:

- Quelle est la valeur des équipements, des logiciels et surtout des informations?
- Quel est le coût et le délai de remplacement?
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs).
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société?

1.3) Établissement d'une politique de sécurité

Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables. Voici quelques éléments pouvant aider à définir une politique :

- Quels furent les coûts des incidents informatiques passés?
- Quel degré de confiance pouvez vous avoir envers vos utilisateurs interne?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante?
- Y a-t-il des informations importantes sur des ordinateurs en réseaux? Sont-ils accessibles de l'externe ?
- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur?
- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations (ex: loi « informatique et liberté », archives comptables)?

1.4) Éléments d'une politique de sécurité

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties :

- **Défaillance matérielle :** Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.
- **Défaillance logicielle :** Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulier des logiciels et la visite des sites consacrés à ce type de problèmes peut contribuer à en diminuer la fréquence.
- **Accidents (pannes, incendies, inondations…) :** Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :

- Disques RAID pour maintenir la disponibilité des serveurs.
- Copie de sécurité via le réseau (quotidienne)
- Copie de sécurité dans un autre bâtiment (hebdomadaire)

La disposition et l'infrastructure des locaux peuvent aussi fournir une protection intéressante. Pour des sites particulièrement important (site informatique central d'une banque…) il sera nécessaire de prévoir la possibilité de basculer totalement et rapidement vers un site de secours (éventuellement assuré par un sous-traitant spécialisé). Ce site devra donc contenir une copie de tous les logiciels et matériels spécifiques à l'activité de la société.

- **Erreur humaine :** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.
- **Vol via des dispositifs physique (disques et bandes) :** Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.
- **Virus provenant de disquettes :** Ce risque peut-être réduit en limitant le nombre de lecteur de disquettes en service. L'installation de programmes antivirus peut s'avérer

une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mises à jour.

- **Piratage et virus réseau :** Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit.

2) Failles de sécurité sur Internet

En entreprise, c'est le réseau local qui est connecté à Internet. Il est donc indispensable de contrôler les communications entre le réseau interne et l'extérieur. De plus une formation du personnel est indispensable (règles de sécurité, déontologie, attention aux participations aux forums qui sont archivées ...).

Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers. Une menace qui a sensiblement augmenté au cours de ces dernières années, nous indique la dernière étude du *Computer Security Institute*, un institut professionnel de San Francisco qui réalise chaque année un sondage auprès des entreprises en collaboration avec le FBI. Dans cette étude, plus de 40 % des sociétés interrogées ont déclaré que des intrus s'étaient introduits dans leurs systèmes depuis l'Internet, 38 % des sociétés ont détecté des attaques de type "déni de service", et 94 % ont été infectées par un virus en 2000.

D'autre part, votre sécurité peut dépendre d'autres entreprises dont vous pensez, parfois à tort, qu'elles ont assuré leur propre sécurité. Alors que le gouvernement et les forces de l'ordre cherchent à interpeller les intrus, les sociétés ne se préoccupent trop souvent que de relancer leurs réseaux après une attaque. « Le secteur privé ne cherche pas à savoir qui est responsable, tout ce qui intéresse les entreprises, c'est que l'attaque cesse. ».

2.1) Définitions

2.1.1) *IP spoofing*

Usurpation d'adresse IP, on fait croire que la requête provient d'une machine autorisée. Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

2.1.2) *DNS spoofing*

Pousse un serveur de DNS à accepter l'intrus. Solution : séparer le DNS du LAN de celui de l'espace public.

2.1.3) *Flooding*

Raid massif de connexions non terminées.

2.1.4) *Smurf*

Saturation de la bande passante.

2.1.5) *Web bug*

Un mail publicitaire est envoyé en HTML (même si l'apparence est normale) avec une image transparente gif d'un pixel par un lien du type :

<img src="http://www.serveur.xx/image.gif ?email=utilisateur@adresse">

Si le courrier est ouvert pendant la connexion, la requête de téléchargement de l'image vient confirmer la lecture du message et la validité de votre adresse.

Conseil : ne pas valider l'ouverture automatique du format HTML ou ne pas ouvrir ses courriers en ligne.

2.1.6) *Hoax (rumeur)*

Un « hoax » est une rumeur que l'on transmet par mail. Ces rumeurs colportent souvent des problèmes de sécurité soit disant découverts par des services officiels ou célèbres… Elles peuvent causer un véritable préjudice à certaines sociétés et de toute façon encombrent le réseau. Avant de retransmettre un tel message il est prudent de vérifier son authenticité.

2.1.7) *Hacker et cracker*

Il existe une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, dont l'histoire remonte aux premiers mini-ordinateurs multi utilisateurs, il y a quelques dizaines d'années, et aux premières expériences de l'ARPAnet.

Les membres de cette culture ont créé le mot ***"hacker"***. Ces informaticiens sont généralement discrets, anti-autoritaristes et motivés par la curiosité.

Il y a un autre groupe de personnes qui s'autoproclament des "hackers". Ces gens (principalement des adolescents de sexe masculin) prennent leur pied en s'introduisant à distance dans les systèmes informatiques et en piratant les systèmes téléphoniques, généralement à l'aide d'outils écrit par d'autres et trouvés sur Internet. Ils publient sur alt.2600. Les vrais hackers appellent ces gens des ***"crackers"*** et ne veulent rien avoir à faire avec eux. Les vrais hackers pensent que les crackers sont des gens *paresseux, irresponsables et pas très brillants*.

2.2) Principales attaques

2.2.1) *Virus*

Les virus sont des exécutables qui vont exécuter des opérations plus ou moins destructrices sur votre machine. Les virus existent depuis que l'informatique est née et se propageaient

initialement par disquettes de jeux ou logiciels divers... Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions,
- Ouverture sans précautions de documents contenant des macros,
- Pièce jointe de courrier électronique (exécutable, script type vbs…),
- Ouverture d'un courrier au format HTML contenant du javascript exploitant une faille de sécurité du logiciel de courrier (normalement javascript est sans danger).
- Exploitation d'un bug du logiciel de courrier (effectuer régulièrement les mises à jour).

Les virus peuvent être très virulent mais ils coûtent aussi beaucoup de temps en mise en place d'antivirus et dans la réparation des dégâts causés. On peut malheureusement trouver facilement des logiciels capables de générer des virus et donc permettant à des « amateurs » (aussi appelés *crackers*) d'étaler leur incompétence.

La meilleure parade est l'utilisation d'un antivirus à jour et d'effectuer les mises à jour des logiciels (pour éviter l'exploitation des bugs).

2.2.2) *Déni de service (DoS)*

Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources.

2.2.3) *Écoute du réseau (sniffer)*

Il existe des logiciels qui, à l'image des analyseurs de réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible *(Network packet sniffing).* C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en « broadcast » sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

L'utilisation de *switches* (commutateurs) réduit les possibilités d'écoute mais en inondant le commutateur, celui-ci peut se mettre en mode « HUB » par « sécurité »

La meilleure parade est l'utilisation de mot de passe non rejouable, de carte à puce ou de calculette à mot de passe.

2.2.4) *Intrusion*

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique et chantage

Le principal moyen pour prévenir les intrusions est le coupe-feu ("firewall"). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés. Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log » (traces) est complémentaire.

2.2.5) *Cheval de Troie*

L'image retenue de la mythologie est parlante; le pirate, après avoir accédé à votre système ou en utilisant votre crédulité, installe un logiciel qui va, à votre insu, lui transmettre par Internet les informations de vos disques durs. Un tel logiciel, aussi appelé troyen ou *trojan*, peut aussi être utilisé pour générer de nouvelles attaques sur d'autres serveurs en passant par le votre. Certains d'entre eux sont des « key logger » c'est-à-dire qu'ils enregistrent les frappes faites au clavier.

La première mesure de protection face aux attaques, et de sécuriser au maximum l'accès à votre machine et de mettre en service un antivirus régulièrement mis à jour. Un nettoyeur de troyens peut aussi s'avérer utile.

Attention : sous Windows, un partage de fichiers actifs et trop permissif offre les mêmes possibilités sans que le visiteur n'a besoin d'installer un logiciel.

2.2.6) *« social engeneering »*

En utilisant les moyens usuels (téléphone, email…) et en usurpant une identité, un pirate cherche à obtenir des renseignements confidentiels auprès du personnel de l'entreprise en vue d'une intrusion future. Seule une formation du personnel permet de se protéger de cette attaque.

2.3) Espionnage

2.3.1) *L'homme du milieu*

Lorsqu'un pirate, prenant le contrôle d'un équipement du réseau, se place au milieu d'une communication il peut écouter ou modifier celle-ci. On parle alors de « l'homme du milieu » *(man in the middle)*. Les points sensibles permettant cette technique sont :

- **DHCP:** Ce protocole n'est pas sécurisé et un pirate peut fournir à une victime des paramètres réseau qu'il contrôle. Solution : IP fixe.

- **ARP:** si le pirate est dans le même sous réseau que la victime et le serveur (même si commutateur), il peut envoyer régulièrement des paquets ARP signalant un changement d'adresse MAC aux deux extrémités. Solution : ARP statique.
- **ICMP:** Un routeur peut émettre un ICMP-redirect pour signaler un raccourci, le pirate peut alors demander de passer par lui. Solution : refuser ICMP-redirect ou seulement vers des routeurs identifiés.
- **RIP:** Le pirate envoie une table de routage à un routeur indiquant un chemin à moindre coût et passant par un routeur dont il a le contrôle. Solution : nouvelle version de RIP qui intègre une identification des routeurs de confiance.
- **DNS** : par « ID spoofing » un pirate peut répondre le premier à la requête de la victime et par « cache poisoning » il corrompt le cache d'un serveur DNS. Solution : proxy dans un réseau différent des clients, désactivation de la récursivité, vidage du cache DNS régulier.
- **Proxy HTTP:** Par définition un proxy est en situation d'homme du milieu. Une confiance dans son administrateur est nécessaire de même qu'un contrôle du proxy lors de son départ !
- **Virus:** Uu virus, éventuellement spécifique à la victime et donc indétectable, peut écrire dans le fichier « hosts »… Solution : bloquer les .vbs et .exe

2.3.2) *Espiogiciels*

Ces logiciels espions sont aussi appelés ***« spyware ».*** Ils ne posent pas, à priori, de problème de sécurité mais plutôt celui du respect de la vie privée.

Plusieurs logiciels connus se permettent de renvoyer vers l'éditeur des informations concernant l'usage du logiciel mais aussi sur les habitudes ou la configuration de l'utilisateur, et ceci au mépris de la loi « informatique et liberté ». Il s'agit souvent de « freewares » qui trouvent ainsi une source de revenus mais pas toujours !

Exemples : Real Networks (requête vers l'éditeur à chaque insertion de CD-audio avec n° GUID, adresse mail…), CuteFTP…

Une liste des programmes suspects et un outil gratuit (Ad-Aware) est disponible sur www.lavasoft.com.

2.3.3) *Cookies*

Un « cookies » est une chaîne de caractère qu'un serveur dépose sur votre disque dur, via votre navigateur, afin normalement d'accélérer ou d'autoriser votre prochaine visite.

On trouvera des infos sur les cookies à www.epic.org/privacy/internet/cookies Des logiciels permettant le tri des cookies sont disponibles : « cookie crusher » sur www.thelimitsoft.com et « cache & cookiewasher » sur www.webroot.com.

3) Protections

3.1) Formation des utilisateurs

On considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier ...)

- **Discrétion :** la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance de la non divulgation d'informations par ces moyens est indispensable. En effet il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.
- **Virus :** plusieurs études récentes (2001) montrent que 1/3 des utilisateurs ouvriraient encore une pièce jointe d'un courrier nommée « i love you » et que la moitié ouvriraient une pièce nommée « ouvrez-ça » ou similaire… ! L'information régulière du personnel est nécessaire, attention toutefois aux rumeurs (hoax).
- **Charte :** l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle.

3.2) Poste de travail

Le poste de travail reste un maillon faible de la sécurité. Le projet TCPA *(Trusted Computing Platform Alliance)* a pour but d'améliorer sa sécurité en dotant le PC d'une puce dédiée à la sécurité. Elle sera chargée de vérifier l'intégrité du BIOS, du chargement de l'OS, de sauvegarder les clés et certificats (PKI) et connaîtra les protocoles de cryptage (RSA, DES…).

- Plusieurs cartes mère possèdent un cavalier interdisant la reprogrammation du BIOS (flashage), vérifier et mettre en place ce cavalier sur tous les postes !
- Lecteur de disquette : Interdire le Boot disquette (BIOS) voire inhiber complètement le fonctionnement du lecteur.
- Lecteur de CD-ROM : les virus de Boot sont très rares sur CD, mais avec la généralisation des graveurs et la simplification des logiciels de gravure…
- Backup régulier et sécurisé des informations essentielles.
- Multi-boot : à éviter au maximum car la sécurité globale du poste est celle de l'OS le plus fragile et de plus il existe des logiciels permettant de lire sous un OS les autres

partitions en ignorant alors les sécurités (exemple : lecture de fichiers NTFS sans tenir compte des droits).

3.3) Antivirus

Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux.

La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

Deux modes de protection :

- Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.
- Mise en place d'un antivirus sur les points d'entrée/sortie des données du réseau après avoir parfaitement identifiés tous ces points. La rigueur de tout le personnel pour les procédures doit être acquise.

Messagerie : la plupart des virus actuels utilisent ce vecteur de transmission. Les vers s'installent et s'exécutent sans l'intervention de l'utilisateur (exécutable ouvert automatiquement, exploitation d'une faille du logiciel de messagerie…). La protection contre les virus en provenance de la messagerie doit être effectuée, non pas au niveau du poste de travail, mais du serveur. Ainsi certains antivirus agissent au niveau du coupefeu, les deux outils coopérant via le protocole CVP *(Content Vectoring Protocol)* qui normalise leur communication. Les clients de messagerie de Microsoft sont victimes de leurs enrichissements en recourant à Word ou au HTML pour éditer le message, ils rendent possible l'exécution de macrovirus. La parade la plus simple consiste à n'utiliser ces clients de messagerie qu'en mode texte.

Attention, la mise en place d'un antivirus sur le firewall n'est d'aucun secours en cas de fichiers cryptés !

3.4) Pare-feu (fire wall) ou garde barrière

C'est une machine dédiée au routage entre LAN et Internet. Consulter la RFC2196. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...). Un datagramme non autorisé sera simplement détruit, IP sachant gérer la perte d'information. Une translation d'adresse pourra éventuellement être effectuée pour plus de sécurité (protocole NAT *Network Address Translation* RFC 1631+2663). Attention : un firewall est inefficace contre les attaques ou les bévues situées du coté intérieures et qui représentent 70% des problèmes de sécurité !

3.4.1) Architecture classique

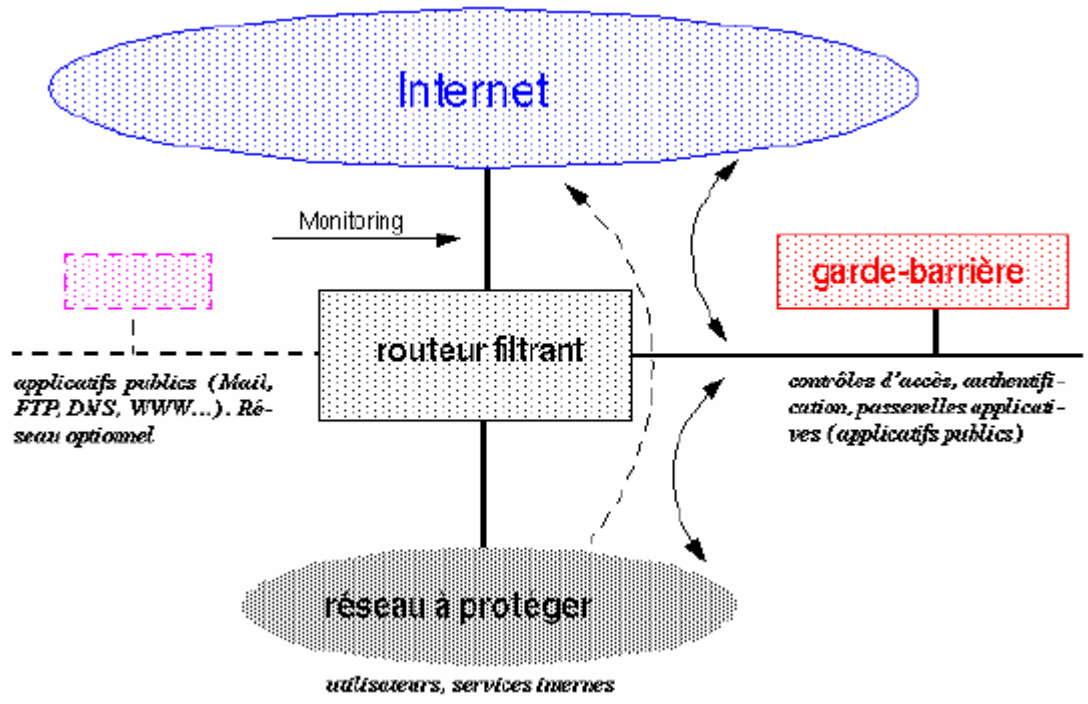


Figure 1.2.8 *: Architecture classique du pare feu*

3.4.2) Architecture concentrée

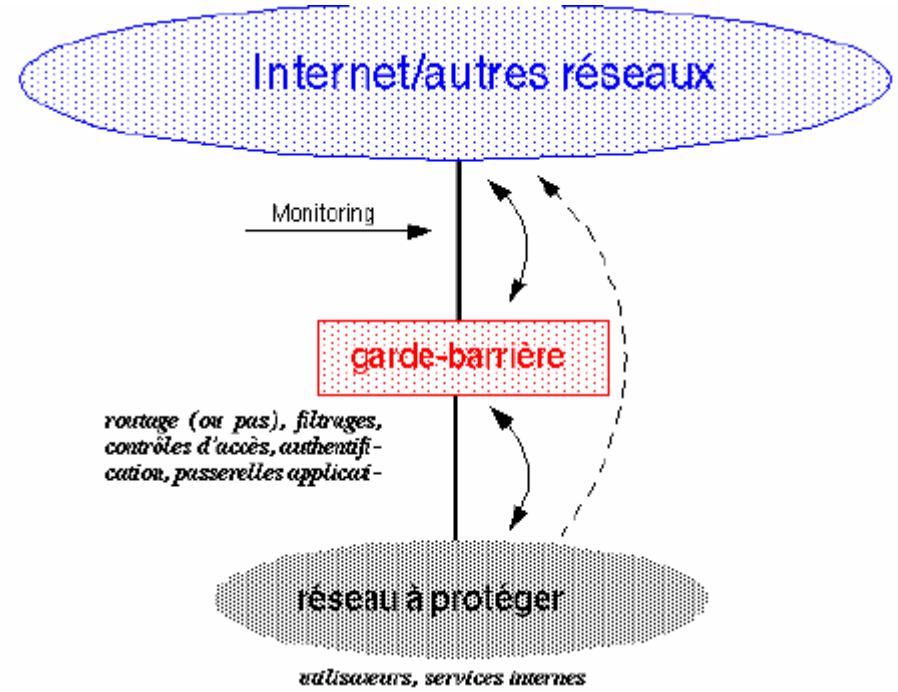


Figure 1.2.9 *: Architecture concentrée du pare feu*

3.4.3) Logiciels

Par sécurité on désactivera tous les services inutiles (TELNET, ...) et on fermera tous les ports TCP/UDP inutilisés (ex TCP 139=Netbios pour partage de dossiers ! ...) (Un outil de protection personnel gratuit « zonealarm » est proposé par www.zonelabs.com ou bien « kerio personnal » chez www.kerio.com) En logiciel libre on utilisera « Ipchain » (noyau Linux) ou « Netfilter » (similaire au produit de checkpoint). Pour ceux qui tournent sous MacOS, il en existe aussi quelques uns dont « Netbarrier » (intego.com) et « DoorStop » (opendoor.com).

Dans certains sites on place les serveurs liés aux services Internet dans une « zone démilitarisée » (DMZ), les accès en provenance d'Internet ne peuvent voir que ces machines et les utilisateurs de l'entreprise doivent passer par les machines de la DMZ pour accéder à Internet.

Au niveau réseau local, un programme correctement écrit (sniffer) peut quand même observer le trafic et saisir noms et mots de passe qui circuleraient sur le réseau à diffusion (Ethernet via Hubs) !

Dans le domaine commercial, les logiciels firewall les plus réputés sont VPN de checkpoint et e-trust de Computer Associates. Il existe aussi des boîtiers « tout compris » du type firebox de Watchguard ou Instagate de Techniland.

3.5) VPN

Le terme VPN (Virtual Private Network) ou réseau privé virtuel est un système qui permet de relier deux réseaux distants à travers Internet. Il est ainsi possible de faire communiquer ces deux réseaux comme si ils étaient connectés directement ensemble.

Le principe de base est que les données du VPN ne peuvent pas être accédées par les autres utilisateurs du réseau global. Ceci est en principe obtenu par cryptage des communications, mais aussi par filtrage et authentification des machines qui s'y connectent. Ainsi, dans le quasi totalité des implémentations d'un VPN, un cryptage est rajouté entre les deux connectiques mais un VPN n'est pas forcément crypté.

3.5.1) Principe de La tunnelisation

Un réseau VPN est basé sur le principe de tunnel.

On appel « tunnel », un canal authentifié et éventuellement chiffré entre deux points A et B qui permet l'acheminement du trafic de l'amont de A vers l'aval de B et réciproquement.

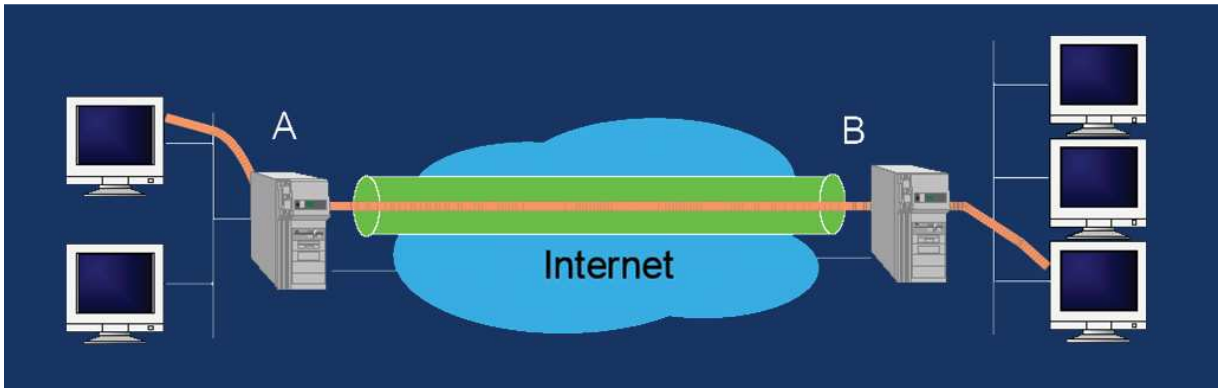


***Figure 1.3.0** : Tunnelisation*

Le tunneling IP est le procédé qui consiste à encapsuler un flux réseau dans les paquets d'un autre flux réseau du type TCP/IP. Il est possible, par exemple, d'encapsuler un flux IPX (réseau NetWare) dans une connexion TCP/IP. Un tunnel IP est un moyen d'assurer l'interconnexion entre deux (ou plus) réseaux dans un réseau plus grand.

Un tunnel IP s'effectue entre 2 machines, qui jouent le rôle de passerelles pour les autres machines de leur réseau respectif.

Le tunneling peut rendre des services de différents ordres :

- ☞ Chiffrement et déchiffrement des données transmises.
- ☞ Compression et décompression des données envoyées dans le tunnel.
- ☞ Offrir l'impression à l'utilisateur de travailler en réseau local (voire sur la même machine)

3.5.2) Principe de L'authentification

C'est la propriété qui assure que seules les entités autorisées ont accès au système. On peut distinguer deux types d'authentifications :

- **L'authentification d'entité ou de l'identification :** par exemple si deux utilisateurs A et B veulent s'assurer de l'identité de l'un ou de l'autre, ils peuvent se poser mutuellement une question à laquelle ils sont les seules à pouvoir répondre

- **L'authentification de l'origine de données :** ce type d'authentification est surtout utile lorsque le message transite par plusieurs réseaux.

Il existe plusieurs technologies permettant d'authentifier, mais les deux méthodes restent les plus répandues :

- **Les certificats digitaux**

Ils sont constitués d'une clé publique et d'un certain nombre de champs d'identification (nom et utilisation du certificat, des informations identifiant le propriétaire de la clé publique, la clé publique proprement dite, une date d'expiration, numéro de série et le nom de l'autorité de certification).

Ils permettent d'assurer la validité de la clé publique. Pour éviter qu'une personne ne se fasse passer pour une autre, un tiers de confiance peut rassembler des informations dignes de foi sur une personne, les ajouter à la clé publique de cette même personne et signer le tout avec sa clé privée. Le fait de signer ce certificat assure l'authentification à la fois des informations, mais aussi de l'entité.

Si une clé publique n'est pas claire, on consultera le certificat de l'autorité jusqu'à aboutir à un certificat portant la signature d'une autorité digne de foi. Un tel certificat permet au titulaire de prouver à tous que la clé publique associée à ce certificat lui appartient et que lui seul pourra déchiffrer les messages que toute personne lui enverra en utilisant cette même clé publique.

On appelle autorité de certification (Certification Autority) le tiers dont le rôle est de distribuer et de gérer les certificats. Elle peut être propriétaire et fournie par le constructeur ou externe. Dans ce dernier cas, c'est société tiers a qui on délègue la gestion de sa clé publique (Verisign, Entrust,…). Les certificats sont composés d'une partie contenant les informations sur l'entité (nom, clé publique, adresse physique, …) et d'une seconde partie concernant la signature. Cette dernière fait état d'un résumé chiffré des ses informations.

Ce résumé chiffré est effectué par un algorithme de hachage (MD5, SHA-1, …) qui retourne un numéro unique, qui à son tour sera chiffré.

Création et distribution d'un certificat

Il existe deux méthodes pour créer ces certificats :

1. L'autorité de certificat crée la paire des clés publique/privée, l'assigne à une entité particulière et inclus la clé publique et l'identité de cette entité dans le certificat. L'entité obtient une copie de la clé privée correspondante après avoir prouver son identité.

2. L'entité crée la paire des clés publique/privée et transmet la clé publique. Dés que la véracité de la clé est assurée, l'autorité crée le certificat.

- **La phrase challenge**

Le processus est semblable à celui utilisé dans le cas des certificats digitaux. La différence réside dans l'absence d'autorité de certification. Les entités doivent elles-mêmes générer leurs certificats digitaux. La signature est alors chiffrée par une phrase challenge commune aux deux entités. Il faut donc nécessairement que celle-ci soit entrée dans tous les équipements désirant communiquer.

3.5.3) Principe du chiffrement

Le chiffrement est basé sur la cryptographie. Son objectif majeur est de transformer des informations dans une forme illisible pour quelqu'un ne détenant pas la méthode de chiffrement. Cette méthode de transformant des informations est réalisée à l'aide d'algorithmes. Les algorithmes utilisent une clé pour contrôler le chiffrement et le déchiffrement. Un message peut être déchiffré si et seulement si sa clé de déchiffrement correspond à la clé de chiffrement.

Les données sont donc cryptées suivant un algorithme et une clé partagée entre les deux extrémités du tunnel. La difficulté à pirater les données dépend essentiellement de l'algorithme choisi et de la longueur de la clé utilisée.

Il existe deux types de chiffrements :

- **Le chiffrement symétrique ou à clé secrète**

Il repose sur le partage d'une clé secrète utilisée pour le chiffrement et le déchiffrement des données à échanger entre deux entités en communication. Avant l'établissement du lien, il faut qu'au préalable les deux entités s'échangent leur clé privée (clé secrète). D'où l'obligation de la gardée confidentiellement. Son inconvénient principal est posé par la transmission de la clé secrète de l'émetteur au destinateur. En effet, si la clé est interceptée par quiconque, celui-ci pourra lire le contenu des messages mais également troubler l'intégrité en ce sens qu'il peut y modifier. Il n'est pas adéquat dans le cas d'un grand nombre d'interlocuteurs susceptibles tous d'échanger des informations. En effet, il faut distribuer dans le cas de N utilisateurs, N*(N-1)/2 clés.

Il faut considérer le temps de chiffrement pour chaque clé qui implique un temps global important.

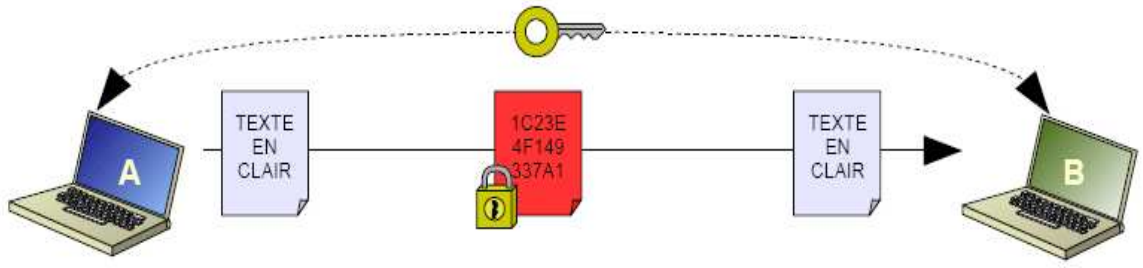


***Figure 1.3.1**: Fonctionnement d'un algorithme de chiffrement symétrique*

- **Le chiffrement asymétrique ou à clé publique**

Il a été développé pour pallier aux insuffisances posées par le chiffrement symétrique. Ce type de chiffrement utilise deux clé différentes, une pour le chiffrement et l'autre pour le déchiffrement. Chaque utilisateur possède son propre couple des clés différentes (secrète et privée). La clé secrète est gardée par son propriétaire qui l'utilise pour sa propre procédure de déchiffrement des messages reçus ou de signatures de message. La clé privée, dérivée de clé sécrète, est rendue publique.

Ainsi donc, pour chaque système de chiffrement asymétrique, le choix d'un couple des clés et la publication de la clé privé par un utilisateur souhaitant recevoir des messages ou émettre des signatures, permettent à tout autre utilisateur de lui envoyer des messages chiffrés et de vérifier ses signatures. Pour émettre un message chiffré, c'est la clé publique du destinataire qui est utilisée et que l'émetteur n'a pas besoin d'aucun paramétrage qui lui soit propre.

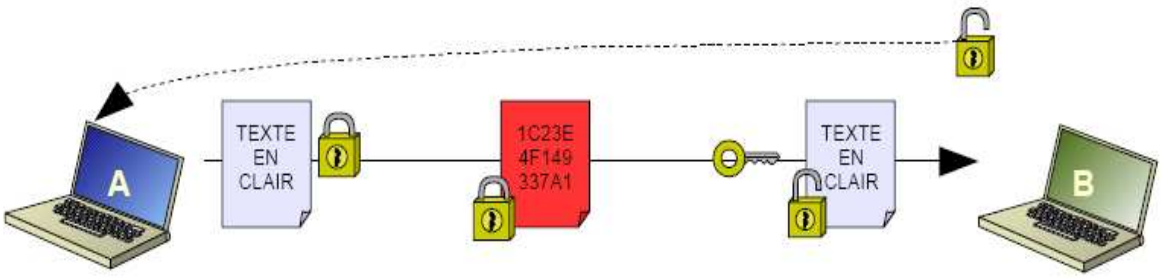


***Figure 1.3.2**: Fonctionnement d'un algorithme de chiffrement asymétrique*

NB : toute clé publique P est dérivée de la clé secrète S, c'est-à-dire qu'à partir de la clé secrète, on peut facilement calculer une clé publique à lui associer .la réciproque est fausse.

Il est à signaler qu'au niveau du chiffrement asymétrique, la transmission de la clé publique P ne pose aucun problème.

3.5.4) Les Protocoles de tunnelisation

3.5.4.1) *Le Protocole PPTP*

PPTP, définit par la Rfc 2637, est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de windows. Ainsi, PPTP est une solution très employée dans les produits VPN à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression.

L'authentification se fait grâce au protocole Ms-Chap de Microsoft qui, après la cryptanalyse de sa version 1, a révélé publiquement des failles importantes. Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap plus sûre. La partie chiffrement des données s'effectue grâce au protocole MPPE (Microsoft Point-to-Point Encryption).

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 définis par le protocole GRE (Generic Routing Encapsulation). Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP.

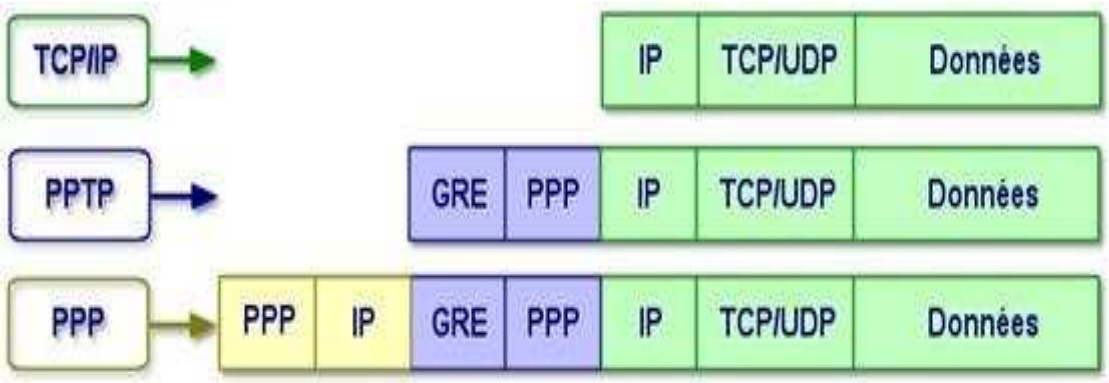


***Figure 1.3.3** : Structure du PPTP et PPP et TCP/IP*

Plusieurs protocoles peuvent être associés à PPTP afin de sécuriser les données ou de les compresser. On retrouve évidement les protocoles développés par Microsoft et cités précédemment. Ainsi, pour le processus d'identification, il est possible d'utiliser les protocoles PAP (Password Authentification Protocol) ou MsChap. Pour l'encryptage des données, il est possible d'utiliser les fonctions de MPPE (Microsoft Point to Point Encryption). Enfin, une compression de bout en bout peut être réalisée par MPPC (Microsoft Point to Point Compression). Ces divers protocoles permettent de réaliser une connexion VPN complète, mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

3.5.4.2) *Le protocole L2TP*

L2TP, définit par la Rfc 2661, est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft, Ascend, 3Com ainsi que d'autres acteurs clés du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et ATM) et 3 (IP). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator) et les serveurs réseau L2TP (LNS : L2tp Network Server). L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'IPSEC et L2TP.

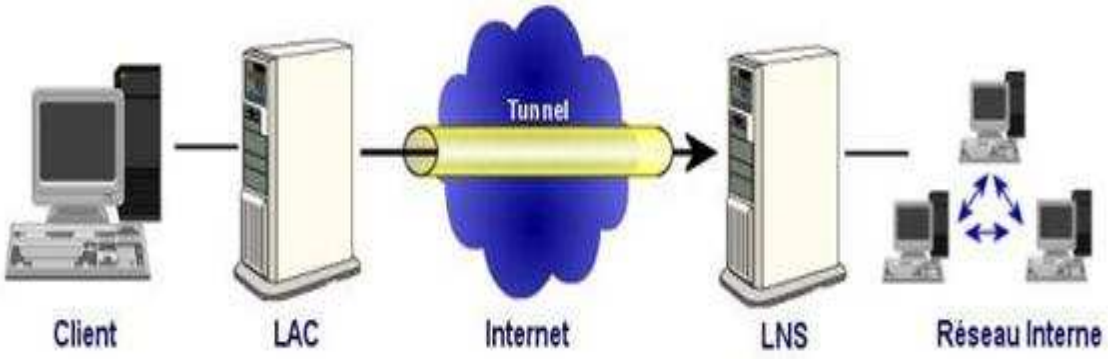


Figure 1.3.4 *: Fonctionnement de protocole L2TP*

3.5.4.2.1) Concentrateurs d'accès L2TP (LAC: L2TP Access Concentrator)

Les périphériques Lac fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le Lac est l'émetteur des appels entrants et le destinataire des appels sortants.

3.5.4.2.2) Serveur réseau L2TP (LNS : L2TP Network Server)

Les serveurs réseau L2TP ou LNS peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le LNS gère le protocole L2TP côté serveur. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local (LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès LAC : ASYNC, RNIS, PPP sur ATM ou PPP sur Relais de Trame. Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification du tunnel.

3.5.4.3) *Le protocole SSL*

Récemment arrivé dans le monde des VPN, les VPN à base de SSL présente une alternative séduisante face aux technologies contraignantes que sont les VPN présentés jusque ici. Les VPN SSL présentent en effet le gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur Internet est implémenté en standard dans les navigateurs

modernes.
SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

SSL a deux grandes fonctionnalités : l'authentification du serveur et du client l'établissement de la connexion et le chiffrement des données durant la connexion.

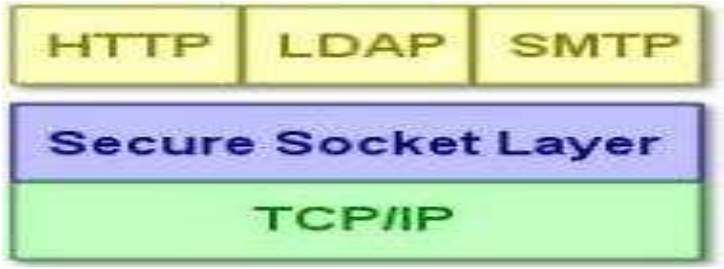


***Figure 1.3.5** : Structure protocole SSL*

❖ Fonctionnement

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérifier la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi la date de validité du certificat et peut également consulter une **CRL** (**Certificate Revocation List**). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ceci est fait de façon à ce que le serveur puisse authentifier le client.

De nombreux paramètres sont échangés durant cette phase : type de clé, valeur de la clé, algorithme de chiffrage.

La phase suivante consiste en l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases du protocole sont :

- Segmentation des paquets en paquets de taille fixe
- Compression (mais peu implémenté dans la réalité)

- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message et de données
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake.
- Ajout d'un en-tête SSL au paquet.

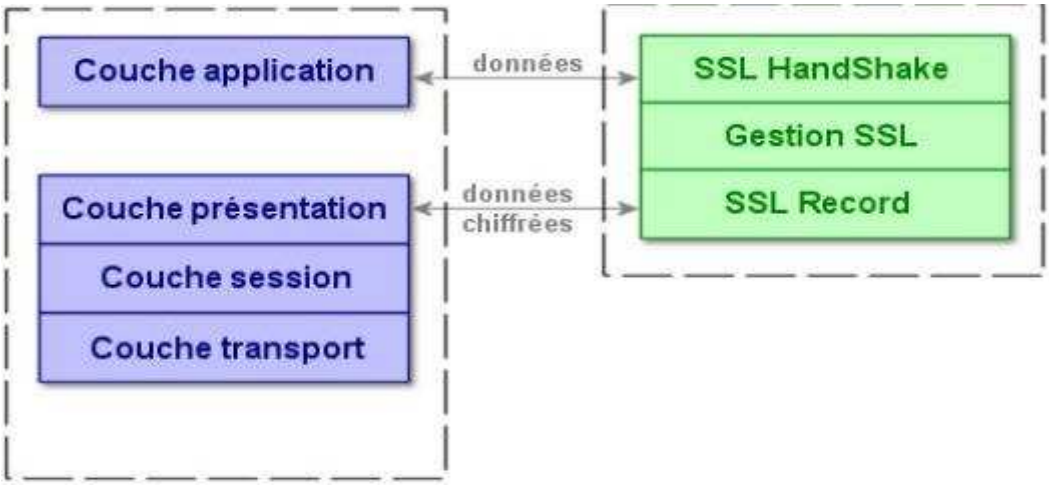


***Figure 1.3.6** : Fonctionnement du protocole SSL*

3.5.4.4) Le protocole IPSec

Internet Protocol Security est le protocole de sécurisation des communications qui s'appuie sur le protocole IP. Il est présent au niveau 3 du modèle OSI. Bien qu'il soit optionnel en IPv4, il est intégré en standard dans le protocole IPv6.

IPSec est employé de deux manières :

- ✓ Mode transport : dans ce mode, les trames sont limitées entre serveurs ou de serveurs à clients (et vice-versa). Ce mode ne peut pas être routé.
- ✓ Mode tunnel : c'est le mode le plus répandu. Il permet de franchir plusieurs réseaux tout en garantissant la sécurité des trames encapsulées.

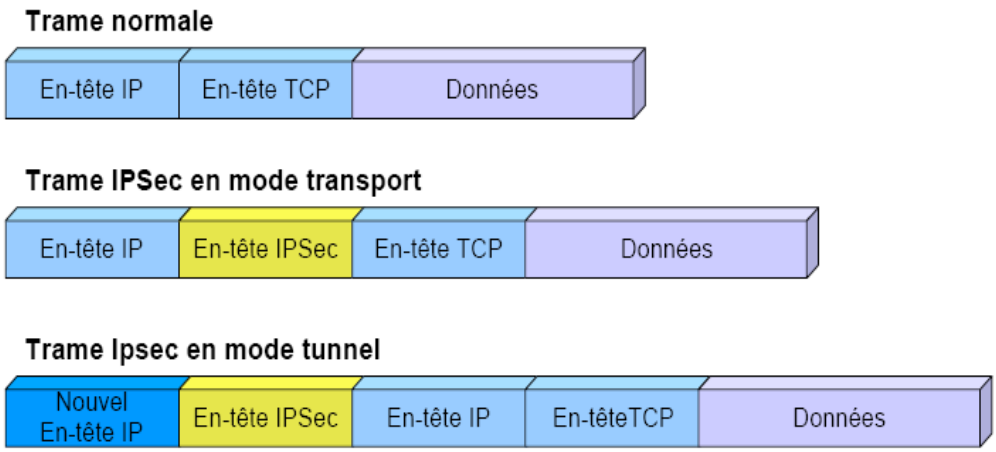


***Figure 1.3.7**: Modes transport et tunnel d'IPSec*

Alors que le mode transport se contente d'insérer un champ IPSec entre l'en-tête IP et l'en-tête TCP, le mode tunnel encapsule toute la trame d'origine dans une nouvelle trame IP (incluant également un en-tête IPSec).

IPSec est basé sur deux protocoles pour la sécurisation des flux : AH et ESP. Ils utilisent tous les deux des méthodes de chiffrement ; toutefois AH ne garantit pas la confidentialité des trames (aucun chiffrement sur le message original n'est fait).

3.5.4.4.1) AH

AH est spécialisé dans l'authentification (mais ne garantit pas l'intégrité des données) et utilise pour cela des mécanismes de hachage.

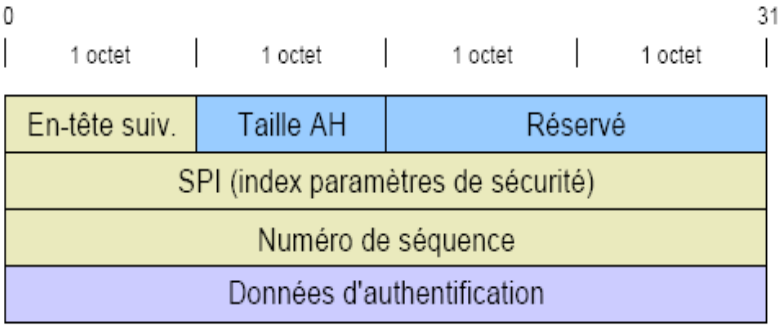


***Figure 1.3.8**: Structure de l'en-tête AH*

La structure AH permet d'éviter le "rejeu" de séquences (grâce aux numéros de séquence) le champ 'en-tête suivant' permet de connaître le numéro du protocole protégé.

3.5.4.4.2) ESP

Ce protocole garantit l'authentification mais aussi la confidentialité et l'intégrité de chaque trame. Il utilise le contrôle d'intégrité (hachage) et le chiffrement des échanges.

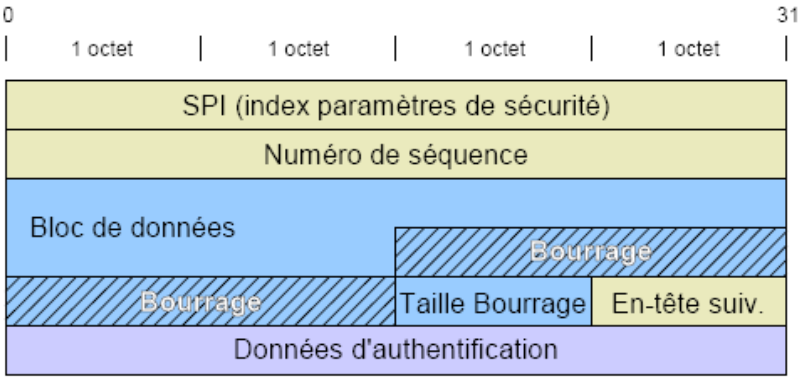


***Figure 1.3.9**: Structure de l'en-tête ESP*

On retrouve les champs "En-tête suivant", "SPI" et "Numéro de séquence" de la structure d'en-tête du protocole AH. Le bloc de données correspond aux données à protéger (confidentialité) avec des champs de "bourrage" (remplissage ou "padding" en anglais) pour permettre l'utilisation d'algorithmes de chiffrement par bloc.

3.5.4.4.3) Fonctionnement d'IPSec

Au niveau de l'authentification, IPSec peut employer HMAC-MD5 ou bien HMAC-SHA-1. Pour la partie chiffrement, il peut s'appuyer sur 3DES-168, CAST-128, DES, Blowfish et AES. Le choix de ces deux paramètres est fait dynamiquement à l'aide du protocole IKE : ce protocole permet l'échange de clé de manière automatique via le protocole UDP (port 500), en utilisant les SA (Security Associations).

IPSec est principalement utilisé en mode tunnel car il permet le chiffrement des données et l'utilisation de réseaux non sécurisés pour la transmission.

3.5.5) Avantages et inconvénients d'un VPN

3.5.5.1) Avantages :

Les VPN présentent essentiellement deux avantages:

- les économies sur les budgets alloués à la connectivité. Ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet;

- La flexibilité. Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.

3.5.5.2) Inconvénients

Parmi les inconvénients des VPN, on peut citer:

- la disponibilité et les performances des VPN dépendent largement des fournisseurs de services et des sous-traitants. L'entreprise ou l'administration utilisant un VPN ne contrôle en effet pas tous les paramètres nécessaires;
- les standards ne sont pas toujours respectés et les technologies VPN restent dépendantes des équipements utilisés. On conseille d'utiliser les équipements du même constructeur pour assurer le bon fonctionnement du VPN d'entreprise.
- la mise en route d'un VPN réclame une forte expertise, et notamment une bonne compréhension de la sécurité informatique et des technologies VPN spécifiques.

BILAN

Avantages de VPN	Inconvénients de VPN
• Coût très faible • Mise on ouvres plus rapide • Sécurité assurer par le chiffrement • Pas de dépendance à la sécurité du FAI • Plus flexible en cas d'évolution et ces nouvelles implémentations • Accès nomade grâce a l'Internet haut débit	• Compétence requise pour la mise en ouvre • Performance non garanties

3.5.6) Les principales solutions VPN du marché

3.5.6.1) Quelques solutions logicielles.

3.5.6.1.1) **Checkpoint** : produit commercial proposant une vaste gamme, implémentation de IPSec et SSL, équilibrage de charge et tolérance aux pannes.
Check Point est le leader mondial de solutions de sécurité réseau pour les entreprises. L'architecture intégrée de Check Point intègre la sécurité réseau, le contrôle du trafic et la gestion d'adresses IP. Les solutions Check Point permettent aux utilisateurs de mettre en place une administration de la sécurité centralisée avec un déploiement distribué à toute l'entreprise. Les produits Check Point intègrent de manière transparente le meilleur des produits de partenaires leaders de l'industrie.

Le VPN-1 de Check Point est un logiciel intégré qui réunit la populaire suite de sécurité FireWall 1 et les technologies sophistiquées des Réseaux privés virtuels (VPN). La pierre angulaire du système de sécurité Check Point, le VPN-1 Pro, rencontre les exigences sévères des RPV Internet, intranet et extranet en garantissant des connexions hautement sécuritaires aux réseaux d'entreprise, aux utilisateurs éloignés et mobiles, aux succursales et aux partenaires commerciaux. Les solutions VPN-1 Pro sont compatibles avec un maximum de plateformes ouvertes et composantes de sécurité pour rester à la hauteur des exigences qualité/prix de compagnies de toutes tailles.

Caractéristiques :

- Assure l'intégration complète avec Firewall-1
- Protège les communications avec IPSec, L2TP, SSL et assure une authentification rigoureuse
- Compatible avec une grande variété de plateformes et de serveurs dédiés
- Offre la meilleure performance sur le marché grâce à SecureXL

Avantages :

- Assure une protection maximale des données corporatives et des communications Internet
- Procure une vaste gamme d'options de déploiement d'accès à distance, et d'authentification des utilisateurs
- Rationalise la gestion de la sécurité
- Assure la flexibilité de la plateforme pour une performance supérieure à meilleur prix

- Permet une très grande extensibilité des RVP et une performance ultra sécuritaire

Inconvénients :

- Solution propriétaire (produit commercial)
- Exige généralement l'installation d'un logiciel client ; il est possible que tous les systèmes d'exploitation client ne soient pas compatibles.
- Les firewalls entre le client et la passerelle peuvent affecter la connectivité (si la politique du pare-feu n'autorise pas IKE ou IPSec).
- La translation d'adresses réseau (NAT) ou les serveurs proxy entre le client et la passerelle peuvent créer des problèmes de connectivité.
- Le client doit être configuré avant d'établir le tunnel.
- Dès qu'un client a un tunnel (PVC, circuit virtuel permanent) dans une entreprise, il peut devenir la cible de pirates (le client distant peut être utilisé pour accéder à l'entreprise, à moins que le risque ne soit atténué par un pare-feu personnel et/ou des contrôles d'accès au niveau de la passerelle VPN).

3.5.6.1.2) **Microsoft** : solutions intégrées à ses produits, implémentation d'IPsec, PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol). Ceci signifie en particulier que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS et sa gestion de droits et de groupe. Cependant comme beaucoup de produit Microsoft la sécurité est le point faible du produit :

Caractéristiques :

- Facilité : VPN sous les produits Microsoft est d'être facile à installer et à mettre en place.
- Architecture Client/Serveur : VPN sous Microsoft est basé sur une architecture client/serveur. Il doit être installé aux deux extrémités du VPN, une est désignée comme serveur, l'autre comme client.
- Modes de sécurité : utilisation des cryptographiques basé sur protocole MsCHAP, MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire. Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

- Tunnenlling : crée tunnel PPTP et ensuite chiffre les données à l'intérieur de celui-ci.

Avantages

- intégrées à ses produits.
- Ne laisse plus filtrer d'informations au sujet du nombre de sessions VPN actives.

Inconvénients :

- Mauvaise gestion des mots de passe dans les environnements mixtes win 95/NT
- Faiblesses dans la génération des clés de session : réalisé à partir d'un hachage du mot de passe au lieu d'être entièrement générées au hasard. (facilite les attaques « force brute »)
- Faiblesses cryptographiques du protocole MsCHAP 1 corrigées dans la version 2 mais aucun contrôle sur cette version n'a été effectué par une entité indépendante.
- Identification des paquets non implémentée : vulnérabilité aux attaques de type « spoofing »

3.5.6.1.3) **OpenVPN** : produit Open Source basé sur OpenSSL, portabilité étendue (Linux, FreeBSD, OpenBSD, Mac OS X, SUN Solaris, Windows 2000/XP/2003), facilité de configuration et d'installation.

Openvpn Créé en 2002, Openvpn est un outil open source utilisé pour construire des VPNs site à site avec le protocole SSL/TLS ou avec des clefs partagées. Son rôle est de "tunneliser", de manière sécurisée, des données sur un seul port TCP/UDP à travers un réseau non sûr comme Internet et ainsi établir des VPNs.

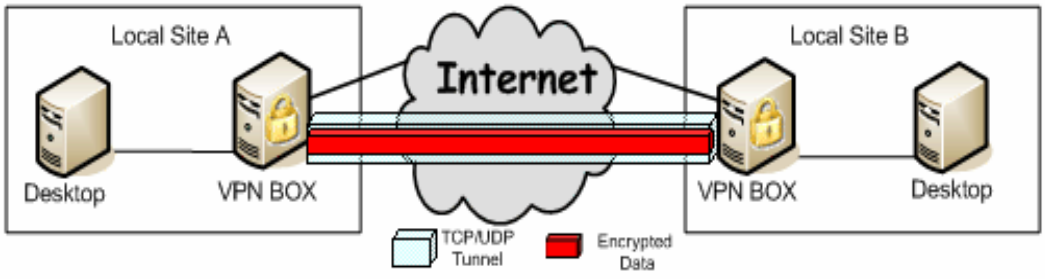


Figure 1.4.0 *: Fonctionnement d'OpenVPN*

Caractéristiques:

- **Facilité :** La grande force d'OpenVPN est d'être extrêmement facile à installer et à configurer, ce qui est rarement le cas pour des outils utilisés pour créer des VPNs.
- **Portabilité :**OpenVPN peut être configuré sur presque toutes les plateformes comme Linux, Microsoft Windows 2000/XP/Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X et Solaris. Les systèmes Linux doivent avoir un noyau 2.4 ou supérieur. Le principe de configuration reste le même quel que soit la plate-forme utilisée.
- **Architecture Client/Server :** OpenVPN est basé sur une architecture client/serveur. Il doit être installé aux deux extrémités du VPN, une est désignée comme serveur, l'autre comme client.
- **Tunnelling :** OpenVPN crée un tunnel TCP ou UDP et ensuite chiffre les données à l'intérieur de celui-ci. Le port par défaut utilisé par OpenVPN est le port UDP 1194, basé sur un assignement officiel de port par l'IANA. Vous pouvez toutefois utiliser n'importe quel autre port et, depuis la version 2.0, un port unique peut être utilisé pour plusieurs tunnels sur le serveur OpenVPN.
- **Modes de sécurité :** Lors de l'utilisation de clefs statiques, les deux passerelles VPN partagent la même clef pour chiffrer et déchiffrer les données. Dans ce cas, les configurations seront très simples mais le problème peut venir du fait qu'il est parfois nécessaire de transmettre la clef (à travers un canal sécurisé bien sûr) à quelqu'un dont vous n'avez pas confiance à l'autre bout du tunnel. L'infrastructure à clef publique (PKI pour Public Key Infrastructure en anglais) est utilisée pour résoudre ce problème. Elle est basée sur le fait que chaque partie possède deux clefs, une clef publique connue de tout le monde et une clef privée tenue secrète. Ce processus est utilisé par OpenSSL, la version gratuite et open source intégrée à OpenVPN, pour authentifier les machines VPN avant le chiffrement des données.

Regardons les avantages des deux modes:

Mode OpenVPN:	Clefs partagées	SSL
Mode de cryptographie:	Symétrique	Asymétrique/Symétrique
Implémentation:	Plus facile	Plus compliquée
Vitesse:	Plus rapide	Plus lente
Consommation CPU:	Plus petite	Plus grande
Echange des clefs:	OUI	NON

Renouvellement des clefs:	NON	OUI
Authentification des passerelles:	NON	OUI

- **Bridging/Routing :** Vous pouvez choisir de construire soit un VPN Ethernet (mode Bridge ou Pont en anglais) ou soit un VPN IP (mode Routage) avec l'aide de respectivement, les pilotes réseaux TAP ou TUN. TAP/TUN sont disponibles sur toutes les plates-formes et sont déjà incorporé dans les noyaux Linux 2.4 ou supérieurs.
- **Options :** Les options d'OpenVPN sont particulièrement importantes. Par exemple le serveur, peut fournir des routes réseaux au client ou peut être utilisé comme serveur DHCP.

Avantages :

- Facile à utiliser, robuste, sécurisé, rapide,portable et configurable sur tous les systèmes d'exploitations.
- Compatible avec le NAT et l'adressage dynamique.
- Hautement configurable
- Evolutif (OpenSSL et pilote TUN/TAP)

Inconvénients :

- Gaspillage d'adresses
- Utilisation du client Windows possibleselon trois cas
  - Utilisateur est aussi un administrateur de son ordinateur
  - Utilisateur connaît le mot de passe d'un administrateur « exécuter sous »
  - Utilisateur ne connaît pas le mot de passe d'un administrateur

3.5.6.2) Quelques solutions matérielles.

Ce sont la plupart du temps des routeurs regroupant des fonctions de VPN. Ce sont aussi des solutions vendues sous forme de boîtiers prêts à configurer. Les fonctionnalités sont plus ou moins riches : Firewall, antivirus, équilibrage de charge.

3.5.6.2.1) Cisco : cluster pouvant atteindre 14 Gbps avec un chiffrement 3DES, convergence des réseaux données, voix, vidéo, à travers un VPN. VPN de Cisco permet d'établir des connexions VPN en IPSec auprès des concentrateurs VPN 3000, des pare-feux PIX/ASA et des routeurs IOS. Les boîtiers Cisco assure en profondeur la

protection des réseaux des petites, moyennes et grandes entreprises. La boîtier VPN le plus vendu au monde et réunit sur une même plateforme une combinaison de technologies éprouvées.

Caractéristiques :

- La Prévention d'Intrusion (IPS),
- Le Filtrage de Contenu (AntiX – technologie en provenance de Trend Micro) ou le VPN SSL, IPsec.

Avantages :

- Possibilité d'intégrer la voix la vidéo et les données
- CONTROLE D'ACCES
- Personnalisation **:** personnalisez le système de sécurité en fonction de besoins d'accès et de la politique de l'entreprise.
- Sécurité avancée **:** technologies en matière de sécurité de contenu, de chiffrement, d'authentification, d'autorisation et de prévention des intrusions.
- Mise en réseau avancée **:** Cisco offre aux utilisateurs nomades et distants un accès parfaitement sécurisé aux ressources de l'entreprise.

Inconvénients.

- La mise en route d'un VPN réclame une forte expertise**,** et notamment une bonne compréhension de la sécurité informatique et des technologies VPN spécifiques.
- Produit commercial
- L'usage de certains protocoles est standardisé
- Mécanismes de sécurité trop nombreux provocant une complexité du système

3.5.6.2.2) Juniper : boîtiers haut de gamme, 6 Gbps en 3DES, jusqu'à 25000 tunnels par boîtier. Les systèmes Secure Access de Juniper Networks sont à la tête du marché des VPN SSL, avec une gamme complète d'appareils d'accès à distance. Les produits VPN SSL de Juniper Networks présentent une grande variété de formats et de fonctions pouvant être combinés pour répondre aux besoins des entreprises de toute taille, des petites structures nécessitant un accès pour les employés distants ou mobiles aux déploiements d'envergure internationale fournissant un accès distant et/ou extranet aux employés, partenaires et clients à partir d'une seule plate-forme. Les VPN SSL de Juniper Networks reposent sur la plate-forme IVE (Instant Virtual Extranet) qui utilise SSL, le protocole de sécurité présent dans tous les navigateurs Web standard. L'utilisation de SSL élimine la nécessité de déployer des logiciels clients et de modifier

les serveurs internes, ainsi que les coûts liés à une maintenance de routine et au support technique. Les appareils VPN SSL Secure Access de Juniper Networks combinent un coût total d'exploitation réduit par rapport aux solutions de clients IPSec traditionnelles et des fonctions de sécurité intégrale uniques. Les méthodes d'accès améliorées permettent aux entreprises de mettre l'accès en service au besoin pour quasiment toutes les ressources, notamment celles sensibles à la latence et à l'instabilité.

Avantages

- Accès sans client aux applications et ressources de l'entreprise
- Une seule plate-forme de pointe pour l'accès distant des employés et des partenaires
- Offres à disponibilité et adaptabilité élevées destinées aux fournisseurs de services
- Sécurité de point final supérieure, contrôle des accès granulaire et prévention contre les menaces et, maintenant, NOUVEAU contrôle coordonné contre les menaces
- Les services sont proposés sur différentes technologies d'accès large bande : hotspots sans fil Wi-Fi 802.11, DSL, câble, Ethernet, ATM, Frame Relay, SONET et fixe sans fil.

Inconvénients :

- Produit commercial
- Nécessite des compétences réseaux avancées pour le paramétrage.

Partie III: Etude de l'existant.

Chapitre 1. Infrastructure existante au niveau de la Direction Générale :

1) Architecture matérielle

La Direction Générale dispose d'un réseau informatique local d'une capacité de 100Mb/s architecturé autour d'un serveur de fichiers, d'impression et active directory qui tourne sous Windows 2003 serveurs, un serveur linux Fidora Core 3 qui contient l'application ADBanking version 2.8 et la basse de donnée (Postgresql), et serveur Linux Fedora 7 contient la version 3.0.1 de l'application ADBanking .Le serveur 2003 est un DELL PowerEdge 2850 Intel ® Xeon ™, CPU 3.40 GHz, 2048 MB Ram, Disk RAID 140Go Hot plug. Les serveurs d'application sont un COMPAQ Proliant DL 380,1 Go Ram, Disk RAID 40 Go Hot plug et Serveur Siemens FUJITSU.

18 postes PC sont connectés au réseau, dont 16 de type Compaq Ipaq i810, pentium3, 128 Mo, 9,7 Go HD et cinq Dell pentium4 , 512 Mo, 80 Go tournant sur Windows 2000 Professionnel et XP.

Les postes sont interconnectés aux serveurs via deux panneaux de brassage par le biais de deux commutateurs (Switch Cisco Catalyst 2950 et Catalyst 3500) lesquels sont reliés entre eux par fibre optique.

Pour les travaux d'impression, les utilisateurs disposent trois imprimantes HP Laserjet 4100 DTN mises en réseau.

La direction générale dispose également de quatre PC portables dont un de marque DELL, (Pentium 3, 128 Mo, 9,7 Go HD tournant sous Windows 2000 professionnel) et trois de marque HP Compaq nx9010, (Pentium4, 256Mo, 37,2 Go HD tournant sur Windows XP Professionnel), accompagnés de trois imprimantes Canon BJC-55 pour ordinateur portable.

Tous les postes disposent d'une connexion Internet. Celle-ci est effectuée via un modem routeur ADSL Wifi marque D-Link DSL-2640T avec une ligne ADSL 1024Mb/s.

Enfin l'institution dispose comme accessoire de sauvegarde un lecteur de bande DLT DELL POWERVAULT VS80 et un graveur DVD LG externe.

A noter que l'ensemble de l'infrastructure informatique est relié à un onduleur (Trace Engineering) afin de pallier les déficiences du courant électrique (les serveurs possèdent un

second onduleur auxiliaire). Enfin les locaux disposent d'un groupe électrogène autonome de 50 KVA.

En résumé, la direction générale dispose d'un réseau local, architecturé autour de :

- Un Serveur (Windows 2003 serveur) Dell power Edge 2850,
- Deux Serveurs (Linux Fedora Core 3 et 7) Compaq Proliant (DL 380) / Serveur Siemens FUJITSU,
- Dix-huit PC Workstations dont seize Compaq Ipaq et deux Dell,
- Quatre PC Portables dont un Dell et trois HP
- Trois Imprimantes HP 4100 en Réseau
- Trois Imprimantes Canon BJC-55 portables
- Un Modem Routeur ADSL 2640T avec une connexion de 1024Mb/s
- Un PBX numérique Forum I18 (Belgacom)
- Deux Switch Cisco Catalyst 2950 et Catalyst 3500.

2) Architectures systèmes

- Linux Fedora
- Windows Server 2003
- Windows 2000 Professionnel
- Windows XP

3) Architecture d'applications

- ADBanking application de la micro finance.
- HIPAYE application qui gère le paiement,
- Western Union,
- Microsoft Office XP, installé sur tous les postes
- F-Secure Anti-virus pour les postes du travail et pour le serveur 2003,

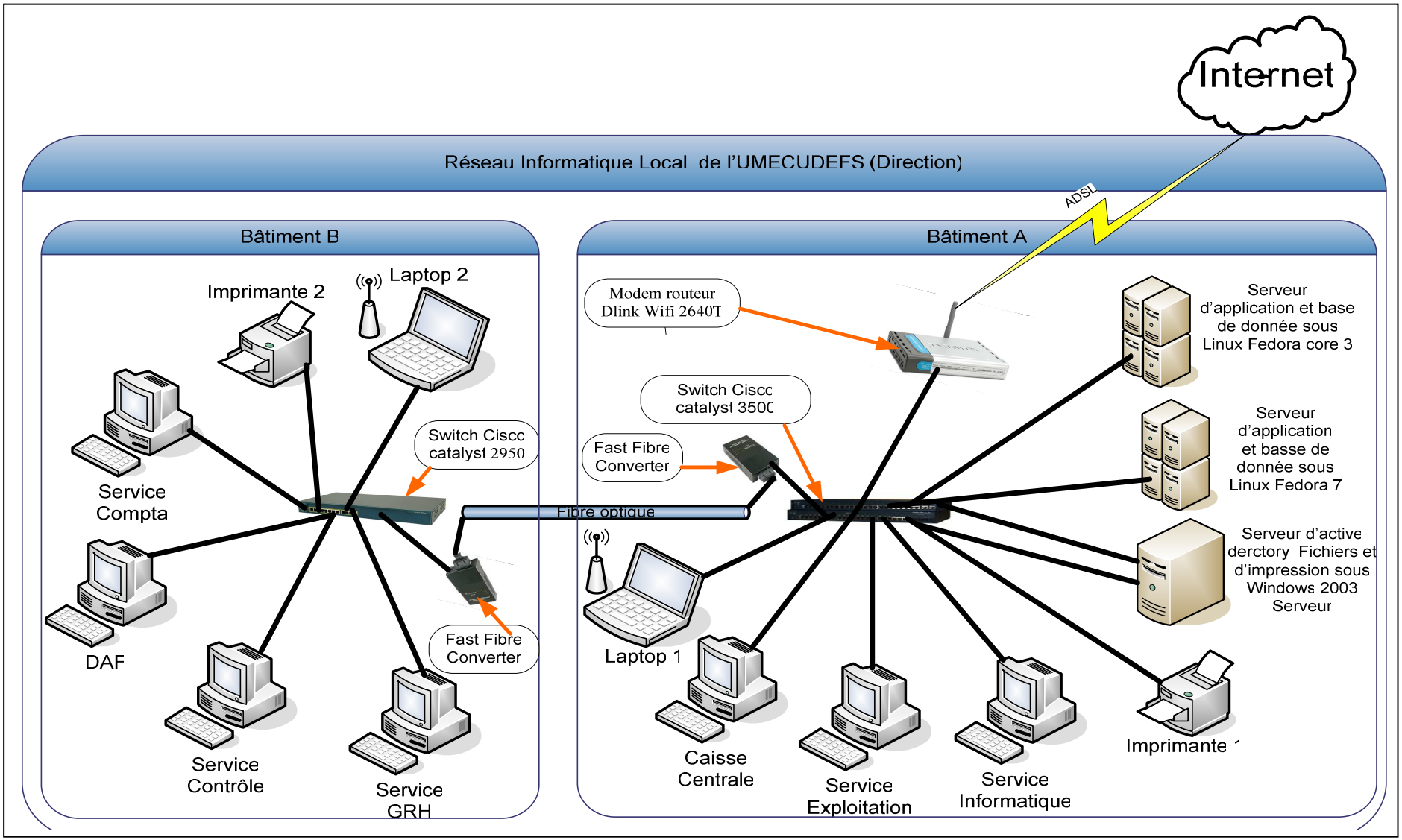
4) Architecture système de gestion de base de données (SGBD)

- PostgreSQL sous linux

5) L'adressage IP

La direction utilise la classe A 10.255.255.XXX avec le masque de sous réseau 255.255.255.0

6) Architecture du réseau informatique de la direction de l'UMECUDEFS



Chapitre 2. Infrastructure existante au niveau des mutuelles :

1) Architecture matérielle

- Un Serveur léger P4 (Linux Fedora core 3 ou Fedora 7),
- Deux ou trois postes de travail (P3 et P4),
- Deux imprimantes laser HP 1018,
- Deux Onduleurs qui protégent le serveur et les machines,
- Switch qui relie les machines entre eux par un réseau léger de type Workgroup,
- Graveur pour les sauvegardes,
- Certaines mutuelles disposent de groupe électrogène,
- Un modem ADSL pour la connexion à l'Internet 512Mb/s (Certaines MECU disposent de Routeur modem ADSL Wifi D-link)

2) Architecture systèmes

- Linux Fedora
- Windows 2000 professionnel
- Windows XP

3) Architecture d'applications

- ADBanking application de la micro finance,
- Western union pour les transferts d'argent,
- Microsoft Office 2003, XP,
- Norton anti-virus 2008,

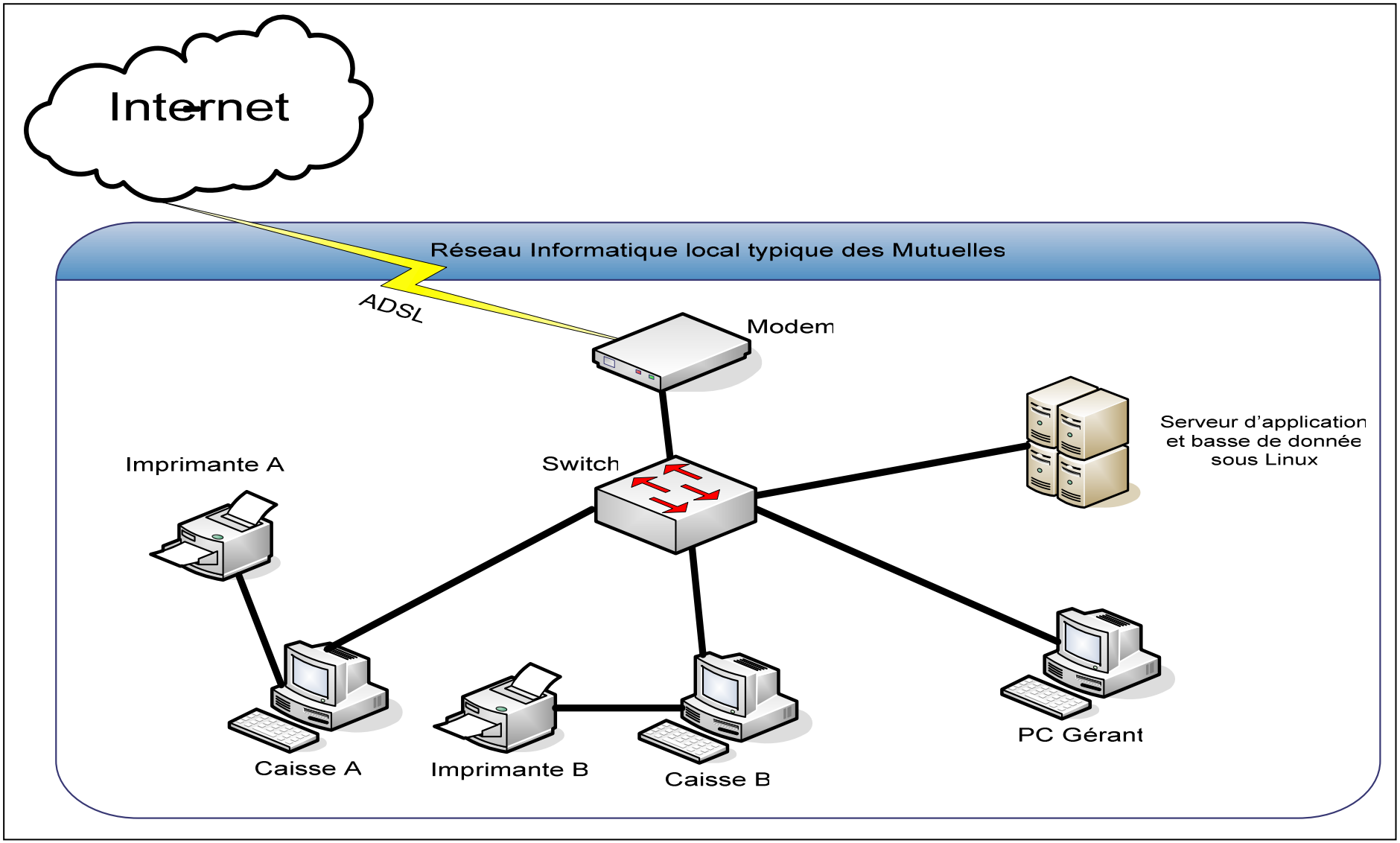
4) Architecture système de gestion de base de données (SGBD)

- PostgreSQL sous linux

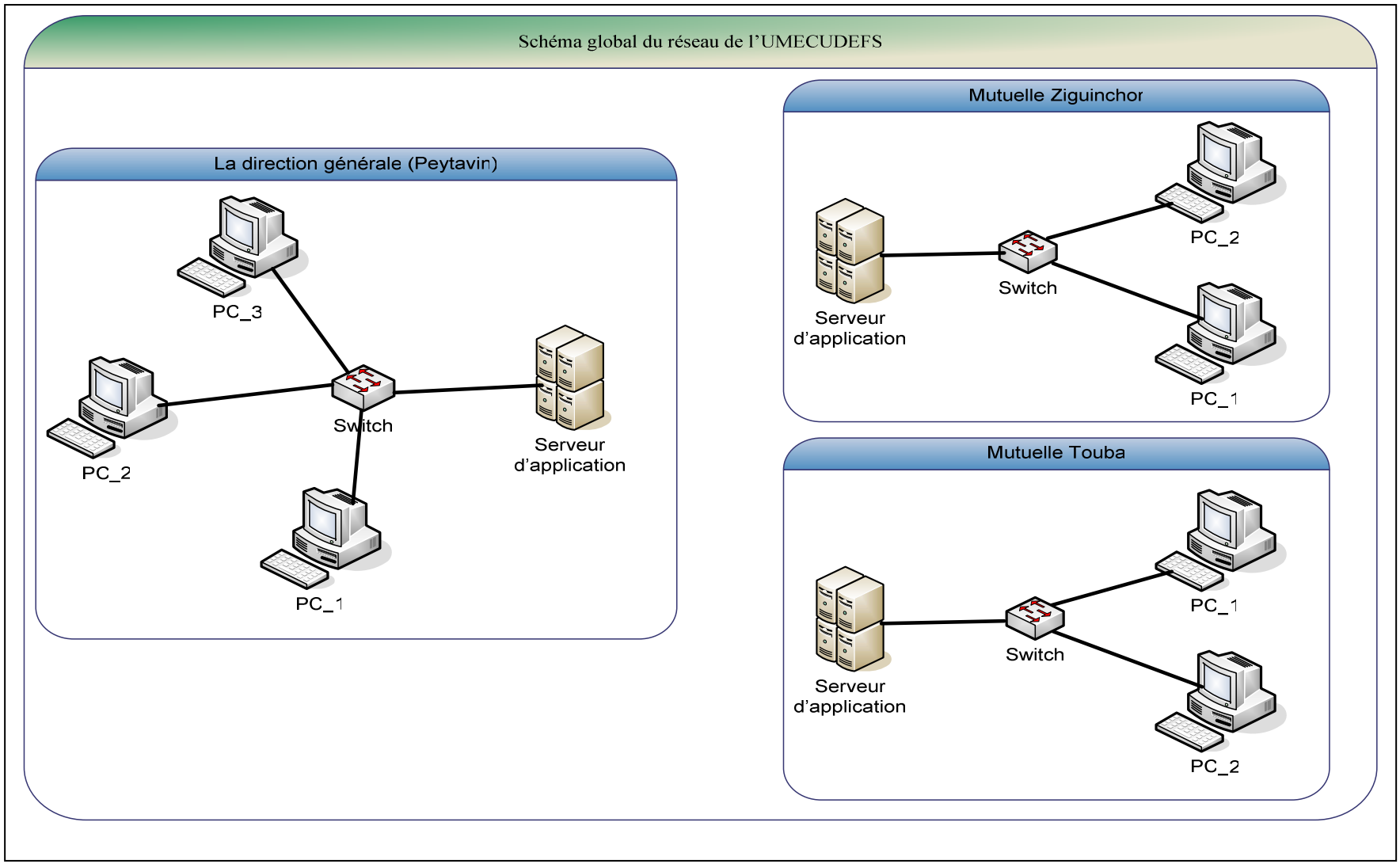
5) L'adressage IP

Certaines mutuelles utilisent la classe A 10.255.255.X avec le masque sous réseau 255.255.255.0 tandis que d'autres utilisent la classe C 192.168.X.X avec le masque 255.255.255.0.

6) Architecture du réseau informatique des mutuelles



Chapitre 3. Existant entre les mutuelles et la direction générale :



1) Fonctionnement entre les mutuelles et le siège:

Le progiciel ADBanking est installé de manière locale dans chaque Mutuelle sans connexion avec la direction générale. Les informations sont envoyées à une fréquence fixée (mensuellement) à la direction par le biais d'un support magnétique CD.

- Solution à coût zéro
- Permet l'individualisation des conditions des produits par mutuelle (montant des pénalités, produits crédit, produits d'épargne…).

2) Critique de l'existant :

- Les avantages de l'informatisation des Mutuelles ne profitent pas à la DG au niveau de la maîtrise du risque global vu le décalage de l'information.
- La maintenance informatique des différentes mutuelles reste impossible à distance et devra. Elle donc se faire uniquement par des techniciens sur place, ce qui exige dès lors un personnel informatique mobile et plus nombreux.
- Risque de dérive du paramétrage dans les Mutuelles (travail de façon non homogène).

Malgré les efforts déployées pour l'informatisation des mutuelles ils demeurés le problème de l'interconnexion de ces derniers à la direction générale. Cette interconnexion avec le siège permettra :

- la sécurité des données
- certains contrôles pourront être effectués à distance de manière systématique.
- La disponibilité d'information sur les expositions et risques globaux de manière non différée
- La possibilité de disposer des états comptables et financiers consolidés à une fréquence plus grande et surtout avec un moindre travail manuel.
- La fidélisation des clients.
- Partages des données et des imprimantes.

Il faut cependant noter que ceci exige la disponibilité d'une connexion continue entre les caisses et la direction générale impliquant des coûts prohibitifs. La prochaine partie explore la solution proposée pour interconnecter l'ensemble des mutuelles avec la direction.

Partie IV: Préconisation technique et organisationnelle

Chapitre 1 : Proposition technique de la solution :

1. Choix de la solution

Apres les comparaisons des avantages et des inconvénients sur l'ensemble des technologies détaillées dans la partie précédente concernant les concepts généraux, notre proposition se porte sur la technologie VPN (Virtual Private Network) en plus le VPN est devenu le meilleur compromis consistant à utiliser Internet pour répondre à un besoin de communication sécurisé et économique de plus en plus grandissant des entreprises.

Et après l'étude des avantages et des inconvénients des solutions matérielles et logicielles du VPN notre solution se base sur OpenVPN comme une solution logicielle implémenter dans le système Linux

2. Politique de la sécurité.

Par rapport à la sécurité nous avons proposé d'implémenter IPCop comme boîtier pare feu pour bien maîtriser notre réseau et d'implémenter l'antivirus F-secure. Dans toutes les caisses de base

Chapitre 2 : Identification des exigences matérielles, logicielles, organisationnelles et opérationnelles pour mettre en place notre solution ;

1) Besoins matériels

- ✓ Un Serveur OpenVPN avec la configuration comme suivant.

- Deux interfaces réseau minimum.
- Microprocesseur à 1.86Ghz
- Mémoire vive 2Go
- 8 Disque dur 72Go RAID
- Graveur DVD+/-RW
- Interfaces (6ports USB, RJ45, Série, parallèle, port souris, port clavier, port graphique, port du gestion à distance iLO2)

- ✓ 36 Boîtiers (machine) OpenVPN comme client et en même temps Pare-feu (IPcop) avec la configuration.

- 2 interfaces réseau minimum.
- Microprocesseur à 1.7Ghz
- Mémoire vive 256Mo
- Disque dur 20Mo
- Lecteur CD-ROM
- Interfaces (4ports USB, RJ45, Série, parallèle, port souris, port clavier, port graphique)
- clavier, écran pour l'installation

2) Besoins logiciels :

- ✓ Linux Fedora 7
- ✓ Openvpn version 2.0.9 pour Windows.
- ✓ IPCop Version 1.4.20

3) Besoins opérationnels :

- ✓ Des liaisons secours RNIS permet de secourir la liaison ADSL en cas de dysfonctionnement.
- ✓ Des formations.
- ✓ Des logiciels du supervisions, d'analyses et détections concernant le réseau et des équipements.

4) Besoins organisationnels :

4.1) Elaboration d'un plan d'adressage IP :

Une option au niveau politique d'adressage adoptée pour le nouvelles réseau de l'UMECUDEFS pourrait être basée sur les techniques de translation d'adresses NAT ou PAT mises en œuvre afin d'interconnecter des réseaux privés (mutuelles et siège) utilisant la RFC1918.

L'utilisation d'adresses privées RFC 1918 (Exemple: 10/16 - 10.x.x.x masque 255.255.0.0) présente un niveau de sécurité supplémentaire pour le Réseau Privé de L'UMECUDEFS.

Cependant la deuxième option du plan d'adressage qui pourrait également être utilisé sur le réseau IP de L'UMECUDEFS sera constitué d'adresses publiques, routables sur Internet.

L'utilisation d'adresses publiques permet aux agents et clients de L'UMECUDEFS de mettre à disposition des services en ligne sur Internet (serveurs WEB, messagerie SMTP, ...).

Dans le cas de l'adressage du réseau métropolitain de l'UMECUDEFS, l'approche utilisée (10/16) est multiple et présente toute les variantes d'utilisation des trois blocs disponibles avec la RFC1918.

L'utilisation d'un adressage privé pour L'UMECUDEFS se justifie pour les raisons suivantes :

- Mise en place d'une politique de sécurité simple et efficace.
- Indépendance de la disponibilité ou de l'indisponibilité d'une nouvelle plage en vue d'une extension du réseau.
- Meilleure visibilité du réseau, dans le cas des connexions aux extrémités, il sera facile de repérer les flux véhiculant l'INTRANET des bureaux de L'UMECUDEFS.
- La difficulté d'avoir des adresses publiques auprès du fournisseur d'accès Internet

4.1.1) Adressages privés :

Pour l'adressage des sites du réseau de L'UMECUDEFS (LAN et équipements), nous proposons la classe A (10.0.0.0) aménagée de la manière ci-après :

10.AA.BBC.DDD

AA : Entité administrative (Direction ou Délégation régionale,…)

BB : numéro de la mutuelle.

C: un différenciateur de l'interface LAN ou Wifi ou bien DMZ.

DDD: numéro du host.

Les valeurs de **C**:

- 1 pour le LAN
- 2 pour le WIFI
- 3 pour le DMZ

Avec cette politique elle va nous faciliter à identifier les mutuelles selon le numéro de la mutuelle, et un abrégé du nom,

De plus, les IP et les noms de machines jouent un rôle dans cette identification.

Exemples :

IP du serveur et du clients OpenVPN interface coté pare feu: **10.AA.BB1.100**

IP du serveur et du client OpenVPN interface coté LAN: **10.AA.BB1.102**

IP du Pare feu IPCop interface LAN : **10.AA.BB1.101**

IP du Pare feu IPCop interface Wifi : **10.AA.BB2.101**

IP de la caisse n°1 : **10.AA.BB1.1**

IP de la caisse n°2 : **10.AA.BB1.2**

Nom du serveur X: **SRXAA-BB** X c'est la fonction de serveur (Web, FTP…)

Nom du serveur OpenVPN: **SRVPNAA-BB**

Nom du client OpenVPN: **CLVPNAA-BB**

Nom du pare feu: **IPCOPAA-BB**

Nom de la caisse n°1 : **CAISSEAA-BB1-1**

Nom de la caisse n°2 : **CAISSEAA-BB1-2**

Nom de la machine Gérant : **GERANTAA-BB1-10**

Nom de la machine Agent de crédit : **AGCREDITAA-BB1-20**

Exemples :

Mutuelle Touba :

Identifiant : Touba12

Entité administrative=2

Numéro : 12

Abrégé : TB

IP du client OpenVPN : **10.2.121.100**

IP du pare feu : **10.2.121.101**

IP de la caisse n°1 : **10.2.121.1**

IP de la caisse n°2 : **10.2.121.2**

Nom du client OpenVPN: **CLVPN2-12**

IP du pare feu : **IPCOP2-12**

Nom de la caisse n°1 : CAISSE**2**-**12**-**1**

Nom de la caisse n°1 : CAISSE**2**-**12**-**2**

Direction :

Identifiant : SIEGE1

Entité administrative=1

Numéro : 1

Abrégé : DG

IP du serveur OpenVPN : **10.1.11.100**

IP du pare feu: **10.1.11.101**

IP de la machine n°2 : **10.1.11.2**

Nom du serveur OpenVPN: **SRVPN1-1**

IP du pare feu : **IPCOP1-1**

Nom de la machine n°1 : **HOSTE1-1-1**

Nom du serveur WEB : UMECUDEFS.COM

4.2.1) Adressages publics

L'UMECUDEFS va acquérir un bloc d'adresses IP publiques pour ses propres besoins

Chapitre 3: Mise en œuvre de la solution :

1) Description de la solution proposée :

Cette architecture s'appuie sur un ensemble des boîtiers (OpenVPN) répartis et sur l'utilisation des technologies basées sur les tunnels SSL. La direction générale sera en relation avec ses différentes mutuelles par des liaisons VPN crées entre le serveur Openvpn et les clients.

Avec l'implémentation du pare feu sous linux pour garantir la sécurité.

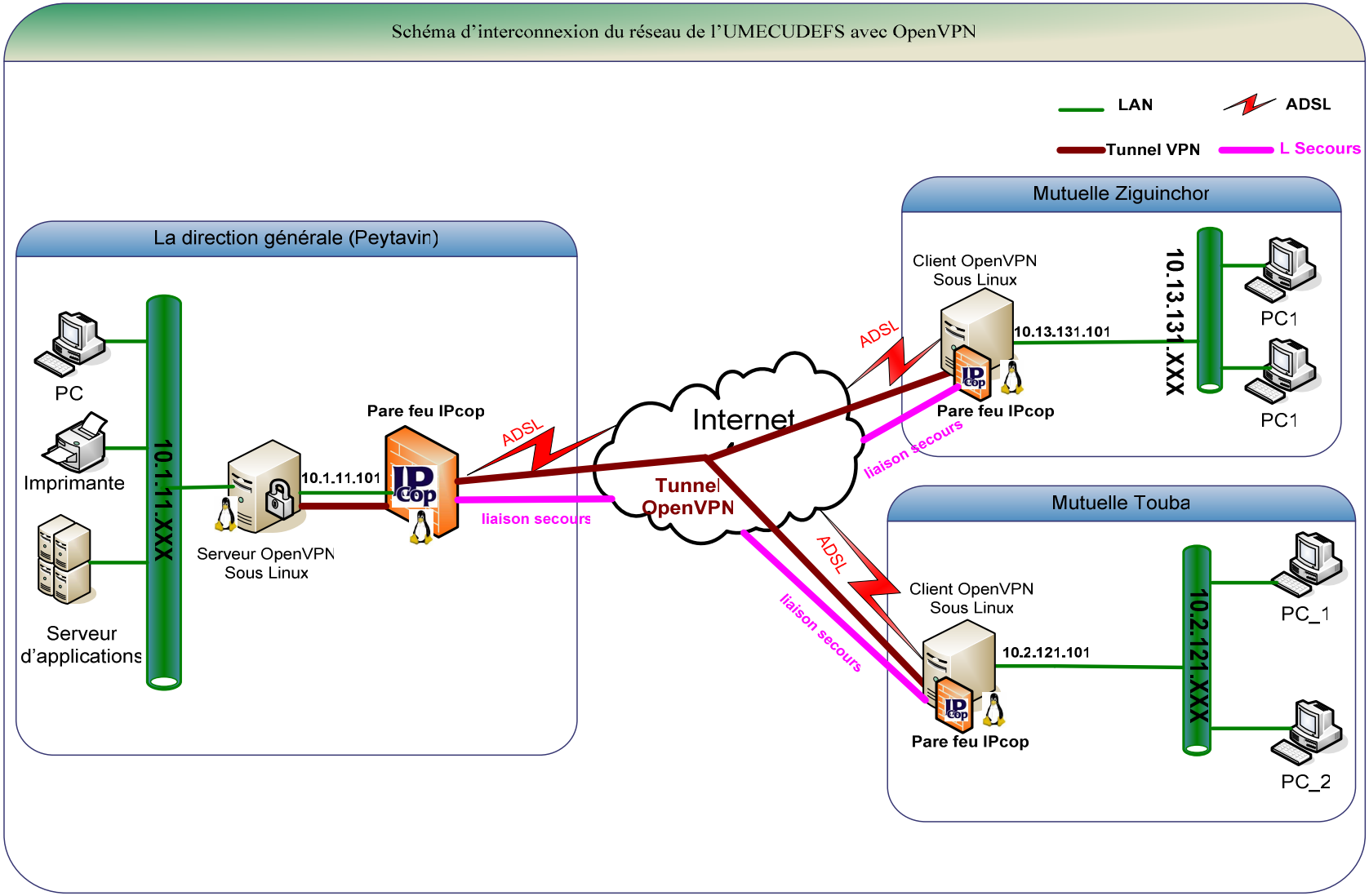


Schéma d'interconnexion du réseau de l'UMECUDEFS avec OpenVPN
LAN
ADSL
Tunnel VPN
L Secours
La direction générale (Peytavin)
PC
Imprimante
Serveur d'applications
10.1.11.XXX
Serveur OpenVPN Sous Linux
10.1.11.101
Pare feu IPcop
ADSL
liaison secours
Internet
Tunnel OpenVPN
Mutuelle Ziguinchor
Client OpenVPN Sous Linux
10.13.131.101
Pare feu IPcop
10.13.131.XXX
PC1
PC1
ADSL
liaison secours
Mutuelle Touba
Client OpenVPN Sous Linux
10.2.121.101
Pare feu IPcop
10.2.121.XXX
PC_1
PC_2
ADSL
liaison secours

2) Mise en œuvre de la solution.

L'objectif est d'interconnecter la direction à 35 sites distants en utilisant le VPN. Les configurations ci-dessous décrivent le cas du Serveur Openvpn (Direction Générale) et d'un Client OpenVPN (Touba) reliées par le réseau IP de Sonatel. Avec l'impléméntation du pare feu IPcop.

2.1) Configuration du Serveur et des Clients OpenVPN

A. Installation du paquetage Openvpn.

Nous allons procéder à la mise en œuvre d'une solution d'interconnexion de sites distants grâce à l'outil openvpn sous fedora 7.
Pour ce faire nous allons utiliser l'incontournable outil de la famille redhat « ***yum*** »
Sur la ligne de commande en tant que super utilisateur, on tape la commande comme à la figure ci
Dessous:

```
[root@UMECUDEFS_SRVPN1 ~]# yum install openvpn_
```

Voilà il nous propose un autre outils très intéressant qui assure la compression des données sous le tunnel pour mieux gagner en vitesse de transmission: il s'agit de l'outil « **lzo** », nous verrons cet outils dans les fichiers de configuration un peu plus tard

```
--> Running transaction check
---> Package openvpn.i386 0:2.1-0.19.rc4.fc7 set to be updated
--> Processing Dependency: liblzo2.so.2 for package: openvpn
--> Restarting Dependency Resolution with new changes.
--> Running transaction check
---> Package lzo.i386 0:2.02-2.fc6 set to be updated

Dependencies Resolved

================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 openvpn                 i386       2.1-0.19.rc4.fc7  fedora            356 k
Installing for dependencies:
 lzo                     i386       2.02-2.fc6       fedora             63 k

Transaction Summary
================================================================================
Install      2 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 419 k
Is this ok [y/N]: _
```

Voilà, donc on tape « y »

Alors en général ***yum*** installe et démarre les programmes, nous allons voir dans les sockets démarrés du système.

```
Remove       0 Package(s)

Total download size: 419 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): openvpn-2.1-0.19.r 100% |=========================| 356 kB    00:09
(2/2): lzo-2.02-2.fc6.i38 100% |=========================|  63 kB    00:01
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 4f2a6fd2
Importing GPG key 0x4F2A6FD2 "Fedora Project <fedora@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY-fedora
Is this ok [y/N]: y
Importing GPG key 0xDB42A60E "Red Hat, Inc <security@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY
Is this ok [y/N]: y
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: lzo                  ########################### [1/2]
  Installing: openvpn              ########################### [2/2]

Installed: openvpn.i386 0:2.1-0.19.rc4.fc7
Dependency Installed: lzo.i386 0:2.02-2.fc6
Complete!
[root@UMECUDEFS_SRVPN1 ~]# _
```

```
Is this ok [y/N]: y
Downloading Packages:
(1/2): openvpn-2.1-0.19.r 100% |=========================| 356 kB    00:09
(2/2): lzo-2.02-2.fc6.i38 100% |=========================|  63 kB    00:01
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 4f2a6fd2
Importing GPG key 0x4F2A6FD2 "Fedora Project <fedora@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY-fedora
Is this ok [y/N]: y
Importing GPG key 0xDB42A60E "Red Hat, Inc <security@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY
Is this ok [y/N]: y
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: lzo                         ########################## [1/2]
  Installing: openvpn                     ########################## [2/2]

Installed: openvpn.i386 0:2.1-0.19.rc4.fc7
Dependency Installed: lzo.i386 0:2.02-2.fc6
Complete!
[root@UMECUDEFS_SRVPN1 ~]# netstat -anpe | grep openvpn
[root@UMECUDEFS_SRVPN1 ~]# /etc/init.d/openvpn start
Démarrage de openvpn :                                     [  OK  ]
[root@UMECUDEFS_SRVPN1 ~]# _
```

En effet openvpn tourne, il n'y seulement pas grand choses au niveau des sockets tel a été le comportement après la commande **netstat**.

Je rappelle qu'il nous a déjà installé la librairie **lzo**.

Voyons s'il est quand même au niveau des paquets RPM :

```
(2/2): lzo-2.02-2.fc6.i38 100% |=========================|  63 kB    00:01
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 4f2a6fd2
Importing GPG key 0x4F2A6FD2 "Fedora Project <fedora@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY-fedora
Is this ok [y/N]: y
Importing GPG key 0xDB42A60E "Red Hat, Inc <security@redhat.com>" from /etc/pki/
rpm-gpg/RPM-GPG-KEY
Is this ok [y/N]: y
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: lzo                         ########################## [1/2]
  Installing: openvpn                     ########################## [2/2]

Installed: openvpn.i386 0:2.1-0.19.rc4.fc7
Dependency Installed: lzo.i386 0:2.02-2.fc6
Complete!
[root@UMECUDEFS_SRVPN1 ~]# netstat -anpe | grep openvpn
[root@UMECUDEFS_SRVPN1 ~]# /etc/init.d/openvpn start
Démarrage de openvpn :                                     [  OK  ]
[root@UMECUDEFS_SRVPN1 ~]# netstat -anpe | grep openvpn
[root@UMECUDEFS_SRVPN1 ~]# rpm -qa | grep lzo
lzo-2.02-2.fc6
[root@UMECUDEFS_SRVPN1 ~]# _
```

Exact il est bien là, c'est parfait,

B. Génération des certificats d'authentification,

Nous allons sur ce point générer les certificats et les clés qui vont permettre aux clients et au serveur de s'authentifier mutuellement de telle sorte que personne d'autres que vous ne puisse se connecter au VPN.

Pour ça nous allons se déplacer dans le répertoire **easy-rsa** d'openvpn :

cd /usr/share/openvpn/easy-rsa/

```
[root@UMECUDEFS_SRVPN1 2.0]# cd /usr/share/openvpn/easy-rsa/
[root@UMECUDEFS_SRVPN1 easy-rsa]# ll
total 8
drwxr-xr-x 2 root root 4096 déc 21 14:23 1.0
drwxr-xr-x 2 root root 4096 déc 21 14:23 2.0
[root@UMECUDEFS_SRVPN1 easy-rsa]# cd 2.0/
[root@UMECUDEFS_SRVPN1 2.0]# _
```

```
[root@UMECUDEFS_SRVPN1 2.0]# ll
total 112
-rwxr-xr-x 1 root root   121 avr 25  2007 build-ca
-rwxr-xr-x 1 root root   354 avr 25  2007 build-dh
-rwxr-xr-x 1 root root   190 avr 25  2007 build-inter
-rwxr-xr-x 1 root root   165 avr 25  2007 build-key
-rwxr-xr-x 1 root root   159 avr 25  2007 build-key-pass
-rwxr-xr-x 1 root root   251 avr 25  2007 build-key-pkcs12
-rwxr-xr-x 1 root root   270 avr 25  2007 build-key-server
-rwxr-xr-x 1 root root   215 avr 25  2007 build-req
-rwxr-xr-x 1 root root   160 avr 25  2007 build-req-pass
-rwxr-xr-x 1 root root   430 avr 25  2007 clean-all
-rwxr-xr-x 1 root root  1459 avr 25  2007 inherit-inter
-rwxr-xr-x 1 root root   297 avr 25  2007 list-crl
-rw-r--r-- 1 root root   389 avr 25  2007 Makefile
-rwxr-xr-x 1 root root  7768 avr 25  2007 openssl-0.9.6.cnf
-rwxr-xr-x 1 root root  8230 avr 25  2007 openssl.cnf
-rwxr-xr-x 1 root root 12068 avr 25  2007 pkitool
-rw-r--r-- 1 root root  8864 avr 25  2007 README
-rwxr-xr-x 1 root root   894 avr 25  2007 revoke-full
-rwxr-xr-x 1 root root   180 avr 25  2007 sign-req
-rwxr-xr-x 1 root root  1602 avr 25  2007 vars
-rwxr-xr-x 1 root root   190 avr 25  2007 whichopensslcnf
[root@UMECUDEFS_SRVPN1 2.0]# _
```

```
[root@UMECUDEFS_SRVPN1 2.0]# vi vars
```

Pour les clients et serveur.

Première chose, nous allons modifier les valeurs des variables d'environnement afin de ne pas avoir à répéter les renseignements à fournir à la génération des clé,

Pour cela nous allons éditer le fichier « **vars** » ci dessus :

Voici la liste des paramètres par défaut à modifier, ils sont généralement en bas du fichier sous Fedora .

export KEY_COUNTRY="US"

export KEY_PROVINCE="CA"

export KEY_CITY="SanFrancisco"

export KEY_ORG="Fort-Funston"

export KEY_EMAIL=me@myhost.mydomain

```
# Issue rm -rf warning
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR

# Increase this to 2048 if you
# are paranoid.  This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=1024

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="SN"
export KEY_PROVINCE="SENEGAL"
export KEY_CITY="Dakar"
export KEY_ORG="UMECUDEFS"
export KEY_EMAIL="contact@umecudefs.com"
:wq_
```

Après on sauvegarde de ce fichier, je vais relancer la prise en charge de ces nouvelles variables :

```
# are paranoid.  This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=1024

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="SN"
export KEY_PROVINCE="SENEGAL"
export KEY_CITY="Dakar"
export KEY_ORG="UMECUDEFS"
export KEY_EMAIL="contact@umecudefs.com"
"vars" 64L, 1600C written
[root@UMECUDEFS_SRVPN1 2.0]# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /usr/share/openvpn/eas
y-rsa/2.0/keys
[root@UMECUDEFS_SRVPN1 2.0]# _
```

Il va supprimer le dossier keys (ancien endroit ou il conservait les clés) contenu dans le répertoire qu'il indique,

Donc nous n'avons rien à craindre nous allons lancer le script ***. /clean-all,***

```
[root@UMECUDEFS_SRVPN1 2.0]# ./clean-all
[root@UMECUDEFS_SRVPN1 2.0]# _
```

Alors là nous allons commencer avec une configuration propre.

Voilà

```
[root@UMECUDEFS_SRVPN1 2.0]# ll
total 116
-rwxr-xr-x 1 root root   121 avr 25  2007 build-ca
-rwxr-xr-x 1 root root   354 avr 25  2007 build-dh
-rwxr-xr-x 1 root root   190 avr 25  2007 build-inter
-rwxr-xr-x 1 root root   165 avr 25  2007 build-key
-rwxr-xr-x 1 root root   159 avr 25  2007 build-key-pass
-rwxr-xr-x 1 root root   251 avr 25  2007 build-key-pkcs12
-rwxr-xr-x 1 root root   270 avr 25  2007 build-key-server
-rwxr-xr-x 1 root root   215 avr 25  2007 build-req
-rwxr-xr-x 1 root root   160 avr 25  2007 build-req-pass
-rwxr-xr-x 1 root root   430 avr 25  2007 clean-all
-rwxr-xr-x 1 root root  1459 avr 25  2007 inherit-inter
drwx------ 2 root root  4096 déc 21 14:50 keys
-rwxr-xr-x 1 root root   297 avr 25  2007 list-crl
-rw-r--r-- 1 root root   389 avr 25  2007 Makefile
-rwxr-xr-x 1 root root  7768 avr 25  2007 openssl-0.9.6.cnf
-rwxr-xr-x 1 root root  8230 avr 25  2007 openssl.cnf
-rwxr-xr-x 1 root root 12068 avr 25  2007 pkitool
-rw-r--r-- 1 root root  8864 avr 25  2007 README
-rwxr-xr-x 1 root root   894 avr 25  2007 revoke-full
-rwxr-xr-x 1 root root   180 avr 25  2007 sign-req
-rwxr-xr-x 1 root root  1600 déc 21 14:48 vars
-rwxr-xr-x 1 root root   190 avr 25  2007 whichopensslcnf
[root@UMECUDEFS_SRVPN1 2.0]# _
```

Là il nous a crée un répertoire « **keys** » qui contiendra toute notre famille de clé et mon fichier de **conf** n'est plus zippé (**openssl.cnf**).

Vous pourrez vérifier qu'à présent ce répertoire ne contient que deux fichiers créent par le script **build-all** (index.txt et serial qui sont important pour la génération des certificats server et clients)

```
[root@UMECUDEFS_SRVPN1 2.0]# cd keys/
[root@UMECUDEFS_SRVPN1 keys]# ll
total 4
-rw-r--r-- 1 root root 0 déc 21 14:50 index.txt
-rw-r--r-- 1 root root 3 déc 21 14:50 serial
[root@UMECUDEFS_SRVPN1 keys]# _
```

Là nous allons arriver à la création des certificats.

Première chose nous allons faire une autorité de certification,

Voilà

```
[root@UMECUDEFS_SRVPN1 keys]# cd ..
[root@UMECUDEFS_SRVPN1 2.0]# ./build-ca
Generating a 1024 bit RSA private key
.....................................................++++++
...................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SN]:
State or Province Name (full name) [SENEGAL]:
Locality Name (eg, city) [Dakar]:
Organization Name (eg, company) [UMECUDEFS]:
Organizational Unit Name (eg, section) []:umecudefs_ca
Common Name (eg, your name or your server's hostname) [UMECUDEFS CA]:
Email Address [contact@umecudefs.com]:
[root@UMECUDEFS_SRVPN1 2.0]# _
```

Nous remarquerons que nous avions déjà les valeurs mémorisées dans le fichier « vars ».

Il ne s'agira que de renseigner le nom de la CA (Certification Authority,), pour les valeurs entre crochets appuyer sur Entrée et il prendra la valeur par défaut.

A présent nous venons de créer l'autorité de certification qui est dans le répertoire « keys ».

```
[root@UMECUDEFS_SRVPN1 2.0]# cd keys/
[root@UMECUDEFS_SRVPN1 keys]# ll
total 12
-rw-r--r-- 1 root root 1338 déc 21 15:00 ca.crt
-rw------- 1 root root  887 déc 21 15:00 ca.key
-rw-r--r-- 1 root root    0 déc 21 14:50 index.txt
-rw-r--r-- 1 root root    3 déc 21 14:50 serial
[root@UMECUDEFS_SRVPN1 keys]# _
```

Ce certificat est le certificat racine qui va ensuite nous permettre de créer le certificat serveur et les certificats clients.

Donc la partie publique de ce certificat devrait être déposé au niveau des clients pour qu'ils puissent s'authentifier au niveau du serveur pour qu'ils reconnaissent tous les certificats qui seront crée à partir de cette autorité.

Là nous allons créer le certificat pour le serveur (cette machine même que je dénomme UMECUDEFS_SRVPN1 pour

Le serveur OpenVPN du siège de l'UMECUDEFS).

Ce certificat nous allons l'appeler « UMECUDEFS_SR_VPN», nous allons le signer nous même et ensuite nous allons le générer comme va le montrer cette manipulation.

```
[root@UMECUDEFS_SRVPN1 2.0]# ./build-key-server UMECUDEFS_SR_VPN
Generating a 1024 bit RSA private key
....++++++
.....................................................++++++
writing new private key to 'UMECUDEFS_SR_VPN.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SN]:
State or Province Name (full name) [SENEGAL]:
Locality Name (eg, city) [Dakar]:
Organization Name (eg, company) [UMECUDEFS]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [UMECUDEFS_SR_VPN]:
Email Address [contact@umecudefs.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:p@sswOrd1984*
An optional company name []:
Using configuration from /usr/share/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SN'
stateOrProvinceName   :PRINTABLE:'SENEGAL'
localityName          :PRINTABLE:'Dakar'
organizationName      :PRINTABLE:'UMECUDEFS'
commonName            :T61STRING:'UMECUDEFS_SR_VPN'
emailAddress          :IA5STRING:'contact@umecudefs.com'
Certificate is to be certified until Dec 19 15:31:31 2018 GMT (3650 days)
Sign the certificate? [y/n]:
```

```
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@UMECUDEFS_SRVPN1 2.0]#
```

Très bien il ne reste plus qu'à faire la même opération pour le client, en se servant du script « build-key client » : Le certificat du client nous allons l'appeler « **touba_client1** ».

```
[root@UMECUDEFS_SRVPN1 2.0]# ./build-key client_
```

```
Generating a 1024 bit RSA private key
.........++++++
.....................................++++++
writing new private key to 'client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SN]:
State or Province Name (full name) [SENEGAL]:
Locality Name (eg, city) [Dakar]:
Organization Name (eg, company) [UMECUDEFS]:
Organizational Unit Name (eg, section) []:TOUBA_CLIENT1
Common Name (eg, your name or your server's hostname) [client]:TOUBA_CLIENT1
```

```
A challenge password []:
An optional company name []:
Using configuration from /usr/share/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SN'
stateOrProvinceName   :PRINTABLE:'SENEGAL'
localityName          :PRINTABLE:'Dakar'
organizationName      :PRINTABLE:'UMECUDEFS'
organizationalUnitName:T61STRING:'TOUBA_CLIENT1'
commonName            :T61STRING:'TOUBA_CLIENT1'
emailAddress          :IA5STRING:'contact@umecudefs.com'
Certificate is to be certified until Dec 19 15:54:23 2018 GMT (3650 days)
Sign the certificate? [y/n]:y
```

Voilà nous allons signer le certificat et nous allons ensuite le générer.

```
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@UMECUDEFS_SRVPN1 2.0]#
```

Nous allons maintenant examiner le contenu du répertoire **keys**

```
[root@UMECUDEFS_SRVPN1 2.0]# cd keys/
[root@UMECUDEFS_SRVPN1 keys]# ll
total 64
-rw-r--r-- 1 root root 3935 déc 21 15:33 01.pem
-rw-r--r-- 1 root root 3857 déc 21 15:56 02.pem
-rw-r--r-- 1 root root 1245 déc 21 15:29 ca.crt
-rw------- 1 root root  887 déc 21 15:29 ca.key
-rw-r--r-- 1 root root 3857 déc 21 15:56 client.crt
-rw-r--r-- 1 root root  720 déc 21 15:54 client.csr
-rw------- 1 root root  887 déc 21 15:54 client.key
-rw-r--r-- 1 root root  254 déc 21 15:56 index.txt
-rw-r--r-- 1 root root   20 déc 21 15:56 index.txt.attr
-rw-r--r-- 1 root root   21 déc 21 15:33 index.txt.attr.old
-rw-r--r-- 1 root root  120 déc 21 15:33 index.txt.old
-rw-r--r-- 1 root root    3 déc 21 15:56 serial
-rw-r--r-- 1 root root    3 déc 21 15:33 serial.old
-rw-r--r-- 1 root root 3935 déc 21 15:33 UMECUDEFS_SR_VPN.crt
-rw-r--r-- 1 root root  733 déc 21 15:31 UMECUDEFS_SR_VPN.csr
-rw------- 1 root root  887 déc 21 15:31 UMECUDEFS_SR_VPN.key
[root@UMECUDEFS_SRVPN1 keys]# _
```

Nous voyons que la CA a été générée, la partie certificat serveur a été générée de même que la partie certificat client.

A présent il ne nous reste qu'à créer les paramètres Diffie-helmann :

Diffie-Hellma (D-H) est un algorithme à clé publique utilisé pour assurer un partage de clés secrètes,

```
[root@UMECUDEFS_SRVPN1 2.0]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....+....
.....+.....+...+.....
.....+.....+.....+.....+.
.....+.....+.....+.....+.....+.....
.....+.+.....+.....
.....+.....+....+.....
.....+.....+.....+.....+.....
.....+.....
.+.....+.....+....+.....
.....+.....
.....+.....+.....
.....+.....
+.....+.....+.+.....+.....+.....
.....+.....+....
.....
.....
.....+.....
.....+.....+.....+.....
.....+.....+.....+.....+.....+********
[root@UMECUDEFS_SRVPN1 2.0]#
```

Très bien, là nous avons l'ensemble des informations cryptographiques dont nous avions besoin pour configurer notre VPN .

Nous allons copier l'ensemble de nos informations cryptographiques que nous venons de générer dans le répertoire **keys** dans le repertoire **/etc/openvpn** qui est crée par défaut à l'installation d'openvpn .

```
[root@UMECUDEFS_SRVPN1 2.0]# cp keys/* /etc/openvpn/
[root@UMECUDEFS_SRVPN1 2.0]# _
```

C. Création d'un utilisateur Openvpn qui lancera le service avec des droits restreints.

En général sous LINUX il faut toujours lancer es services avec un utilisateur qui a des droits restreints.

Nous allons ainsi créer notre utilisateur Openvpn avec des droits restreints qui sera chargé de lancer le service de telle sorte que même si on se fait pirater la machine, le pirate n'aura que les droits de cet utilisateur et pas avec les droits root si jamais nous avions lancé le service avec le chef root .

La première des choses à faire est :

```
[root@UMECUDEFS_SRVPN1 2.0]# groupadd openvpn
groupadd : le groupe openvpn existe
[root@UMECUDEFS_SRVPN1 2.0]# _
```

En effet il nous a déjà crée cet utilisateur. Si vous installez openvpn par les

Sources ...ou tout autre sauf ***yum*** ou apt-get ....n'oubliez surtout pas de procéder à ces manipulations.

Ainsi nous pourrons créer l'utilisateur openvpn avec des droits restreint, sans shell de login ni de home directory et le faire appartenir au groupe openvpn que vous aurez crée.

En voici la manipulation.

Nous pouvons d'abord vérifier s'il existe avec :

```
[root@UMECUDEFS_SRVPN1 2.0]# cat /etc/passwd | grep openvpn
openvpn:x:498:498:OpenVPN:/etc/openvpn:/sbin/nologin
[root@UMECUDEFS_SRVPN1 2.0]# _
```

```
[root@UMECUDEFS_SRVPN1 2.0]# useradd -d /dev/null -s /bin/false -g openvpn_
```

Très bien là même si on s'est fait pirater la machine l'utilisateur n'aura même pas de shell de connexion parce que nous sommes vraiment méchant.

D. Configuration et lancement du serveur

Il nous reste a récupérer le fichier de configuration du serveur « **server.conf** » et le mettre dans le répertoire **/etc/openvpn:**

il est par défaut installé dans **/usr/share/doc/openvpn-2.1/sample-config-files**

```
[root@UMECUDEFS_SRVPN1 2.0]# cd /usr/share/doc/openvpn-2.1/sample-config-files/
[root@UMECUDEFS_SRVPN1 sample-config-files]# ll
total 80
-rw-r--r-- 1 root root 3427 avr 25  2007 client.conf
-rw-r--r-- 1 root root 3564 avr 25  2007 firewall.sh
-rw-r--r-- 1 root root   62 avr 25  2007 home.up
-rw-r--r-- 1 root root  639 avr 25  2007 loopback-client
-rw-r--r-- 1 root root  665 avr 25  2007 loopback-server
-rw-r--r-- 1 root root   62 avr 25  2007 office.up
-rw-r--r-- 1 root root   63 avr 25  2007 openvpn-shutdown.sh
-rw-r--r-- 1 root root  776 avr 25  2007 openvpn-startup.sh
-rw-r--r-- 1 root root  131 avr 25  2007 README
-rw-r--r-- 1 root root  820 avr 26  2007 roadwarrior-client.conf
-rw-r--r-- 1 root root 1498 avr 26  2007 roadwarrior-server.conf
-rw-r--r-- 1 root root 9970 avr 25  2007 server.conf
-rw-r--r-- 1 root root 1742 avr 25  2007 static-home.conf
-rw-r--r-- 1 root root 1688 avr 25  2007 static-office.conf
-rw-r--r-- 1 root root 1937 avr 25  2007 tls-home.conf
-rw-r--r-- 1 root root 1948 avr 25  2007 tls-office.conf
-rw-r--r-- 1 root root  199 avr 25  2007 xinetd-client-config
-rw-r--r-- 1 root root  989 avr 25  2007 xinetd-server-config
[root@UMECUDEFS_SRVPN1 sample-config-files]# _
```

Là nous allons éditer ce fichier pour y positionner les variables qui vont nous intéresser pour la mise en place du vpn .

Vi server.conf

```
#########################################################
# Sample OpenVPN 2.0 config file for                    #
# multi-client server.                                  #
#                                                       #
# This file is for the server side                      #
# of a many-clients <-> one-server                      #
# OpenVPN configuration.                                #
#                                                       #
# OpenVPN also supports                                 #
# single-machine <-> single-machine                     #
# configurations (See the Examples page                 #
# on the web site for more info).                       #
#                                                       #
# This config should work on Windows                    #
# or Linux/BSD systems.  Remember on                    #
# Windows to quote pathnames and use                    #
# double backslashes, e.g.:                             #
# "C:\\Program Files\\OpenVPN\\config\\foo.key"         #
#                                                       #
# Comments are preceded with '#' or ';'                 #
#########################################################

# Which local IP address should OpenVPN
# listen on? (optional)
"server.conf" 291L, 9970C
```

```
# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp
```

Les principaux paramètres sont les suivants :

port 443

le port par défaut est 1194, nous on y mettra le port 443 qui est un port réservé pour le protocole

https qui traverse rapidement les firewall et les proxy .

En général tous les proxy d'entreprise qui filtre les entrées laissent passer le trafic sur ce port car de toute façon c'est un contenu chiffré que le proxy ne veut pas récupérer .

Proto udp .

évidemment le protocole udp est un bon choix, par défaut il est en udp .

Dev tun

Ok nous nous allons prendre comme interface tun pour tunnel.

Ca ca.crt

cert server.crt

key server.key

Les parametres Diffie hellman

dh dh1024.pem

Exact nous l'avions crée sous ce nom.

C'est une clé de 1024bit , a noter également que nous pouvions bien entendu en faire de 2048 bit pour plus de sécurité mais là c'est un compromis entre performance du tunnel et sécurité du lien .

1024bit est plutôt un bon choix dans notre contexte

A noter qu'on n'a pas besoin de spécifier le chemin d'accès à ces clé et certificats, nous les avions bien copié dans le répertoire courant.

Server 10.1.11.0 255.255.0.0

Nous donnerons cette plage par défaut au serveur.

A chaque fois qu'un client se connectera au vpn, le serveur lui attribuera une adresse Ip contenue dans cette plage.

Bien vérifier en bas du fichier l'utilisation de la librairie **lzo** pour la compression des données.

Comp-lzo

Utiliser l'utilisateur et son groupe openvpn que nous avions crée pour lancer le serveur.

User openvpn

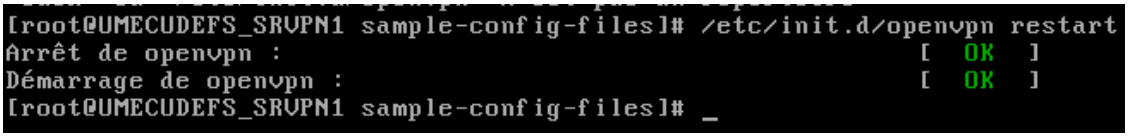
group openvpn

verb 3

Le niveau 3 de log me paraît plutôt bien pour un serveur de production.

Si jamais vous avez des problèmes avec le serveur, il ne démarre pas ....vous pourrez mettre la verbosité maximal qui est de 9 afin d'avoir des log beaucoup plus bavards.

On sauvegarde et on lance le service par le script contenu dans **/etc/init.d/openvpn restrart**



Excellent openvpn est au niveau des sockets démarrés .

Il ne reste plus qu'à s'occuper des clients

E. Configuration du client OpenVPN (Touba)

Alors après avoir installé et configuré notre serveur OpenVPN sous notre fedora nous allons nous intéresser aux clients.

Nous avons opté pour l'installation d'un client sous linux sachant que sous Windows c'est pratiquement la même chose.

Après l'installation d'openvpn avec la commande « ***yum install openvpn*** » dans les boites clients.

On récupère le fichier de configuration du client « ***server.conf*** » et le mettre dans le répertoire **/etc/openvpn:**

Par défaut installé dans **/usr/share/doc/openvpn-2.1/sample-config-files**

```
[root@TOUBA_CLIENT1 ~]# cd /usr/share/doc/openvpn-2.1/sample-config-files/
[root@TOUBA_CLIENT1 sample-config-files]# ll
total 80
-rw-r--r-- 1 root root 3427 avr 25  2007 client.conf
-rw-r--r-- 1 root root 3564 avr 25  2007 firewall.sh
-rw-r--r-- 1 root root   62 avr 25  2007 home.up
-rw-r--r-- 1 root root  639 avr 25  2007 loopback-client
-rw-r--r-- 1 root root  665 avr 25  2007 loopback-server
-rw-r--r-- 1 root root   62 avr 25  2007 office.up
-rw-r--r-- 1 root root   63 avr 25  2007 openvpn-shutdown.sh
-rw-r--r-- 1 root root  776 avr 25  2007 openvpn-startup.sh
-rw-r--r-- 1 root root  131 avr 25  2007 README
-rw-r--r-- 1 root root  820 avr 26  2007 roadwarrior-client.conf
-rw-r--r-- 1 root root 1498 avr 26  2007 roadwarrior-server.conf
-rw-r--r-- 1 root root 9970 déc 21 16:51 server.conf
-rw-r--r-- 1 root root 1742 avr 25  2007 static-home.conf
-rw-r--r-- 1 root root 1688 avr 25  2007 static-office.conf
-rw-r--r-- 1 root root 1937 avr 25  2007 tls-home.conf
-rw-r--r-- 1 root root 1948 avr 25  2007 tls-office.conf
-rw-r--r-- 1 root root  199 avr 25  2007 xinetd-client-config
-rw-r--r-- 1 root root  989 avr 25  2007 xinetd-server-config
[root@TOUBA_CLIENT1 sample-config-files]# _
```

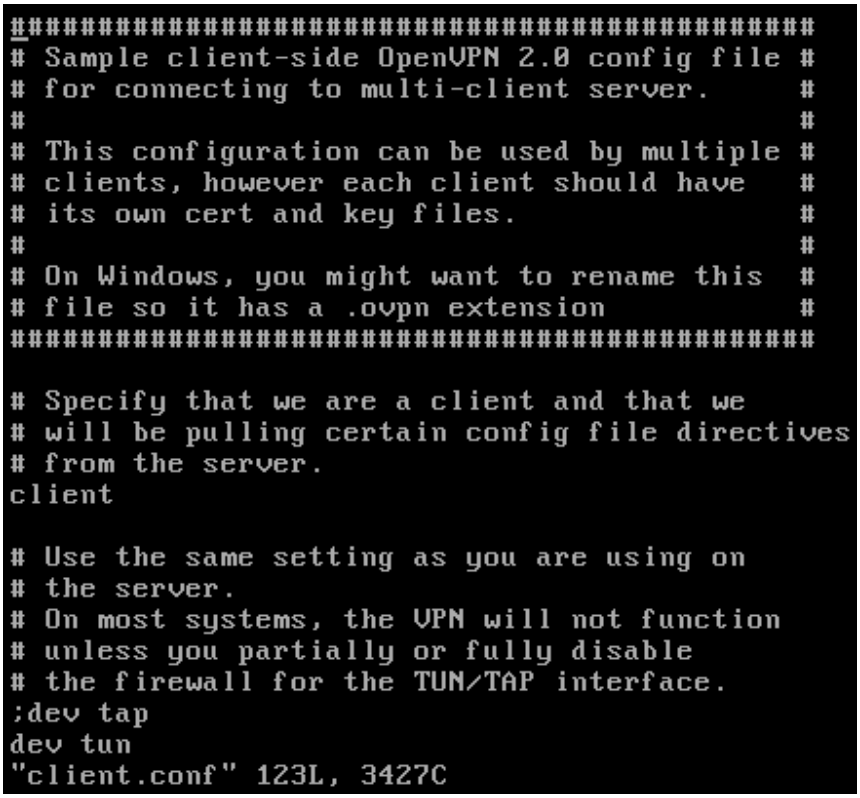
```
[root@TOUBA_CLIENT1 sample-config-files]# cp client.conf /etc/openvpn/
[root@TOUBA_CLIENT1 sample-config-files]# _
```

Il nous faudra également récupérer les informations cryptographiques de la partie client sur le serveur du la direction et les copier dans ce le même répertoire **/etc/openvpn**
On doit copier la Ca, les clés client et le certificat client

```
[root@TOUBA_CLIENT1 openvpn]# ll
total 20
-rw-r--r-- 1 root root 1245 déc 21 20:28 ca.crt
-rw-r--r-- 1 root root 3427 déc 21 20:28 client.conf
-rw-r--r-- 1 root root 3857 déc 21 20:28 client.crt
-rw-r--r-- 1 root root  720 déc 21 20:28 client.csr
-rw------- 1 root root  887 déc 21 20:28 client.key
[root@TOUBA_CLIENT1 openvpn]# _
```

Nous allons éditer le fichier ***client.conf*** avec la commande « ***vi client.conf*** » pour renseigner nos paramètres.

```
[root@TOUBA_CLIENT1 openvpn]# vi client.conf
```



Voilà c'est comme le fichier de conf du serveur sous linux.

Les principaux parametres à modifier :

Client

proto udp, dev tun comme sur le serveur .

```
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote my-server-1 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
```

La partie la plus importante est la ligne « **remote** ».

Alors pour que vous puissiez connecter un client depuis Touba et le serveur se trouvant à Dakar il faut indiquer une adresse IP publique a la place my-server-1.

Et c'est d'ailleurs l'objectif du VPN (Interconnexion de sites distants)

Il est aussi à rappeler que nous pouvons connecter au serveur autant de clients que nous voulons, il faut juste à chaque fois générer les informations cryptographiques au niveau du répertoire easy-rsa du serveur et les déployer par la suite sur le client.

Autre point important il faut obligatoire indiquer l'emplacement des clé et certificats.

Vu que nous les avons dans le repertoire courant, on n'a pas besoin d'indiquer un chemin absolu.

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client.crt
key client.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
```

Ca : certificat de l'autorité de certification

client.crt : le certificat du client

client.key : la clé associée au certificat du client.

De la même manière on vérifie l'utilisation de la **lib lizo** pour la compression des données dans le tunnel VPN .

Voilà on sauvegarde le fichier et on lance le service avec la commande

« /etc/init.d/openvpn restart »

```
[root@TOUBA_CLIENT1 openvpn]# /etc/init.d/openvpn restart
Arrêt de openvpn :                                         [  OK  ]
Démarrage de openvpn :                                     [  OK  ]
[root@TOUBA_CLIENT1 openvpn]# _
```

Très bien là nous pouvons bien voir qu'en l'arrêtant, le client arrive à se connecter et le serveur lui a attribuer l'ip 10.1.11.6

F. La vérification de notre réseau VPN

Voyons voir au niveau des logs du noyau du serveur :

```
er Connection Initiated with 192.168.1.3:3397
Dec 21 21:43:53 TOUBA_CLIENT1 openvpn[2615]: TOUBA_CLIENT1/192.168.1.3:3397 MULT
I: Learn: 10.1.11.6 -> TOUBA_CLIENT1/192.168.1.3:3397
Dec 21 21:43:53 TOUBA_CLIENT1 openvpn[2615]: TOUBA_CLIENT1/192.168.1.3:3397 MULT
I: primary virtual IP for TOUBA_CLIENT1/192.168.1.3:3397: 10.1.11.6
Dec 21 21:43:54 TOUBA_CLIENT1 openvpn[2615]: TOUBA_CLIENT1/192.168.1.3:3397 PUSH
: Received control message: 'PUSH_REQUEST'
Dec 21 21:43:54 TOUBA_CLIENT1 openvpn[2615]: TOUBA_CLIENT1/192.168.1.3:3397 SENT
 CONTROL [TOUBA_CLIENT1]: 'PUSH_REPLY,route 10.1.11.1,topology net30,ping 10,pin
g-restart 120,ifconfig 10.1.11.6 10.1.11.5' (status=1)
```

Au niveau du serveur voici mes différentes interfaces et le serveur ayant pris l'adresse 10.1.11.1

```
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E6:AE:35
          inet adr:192.168.1.7  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::20c:29ff:fee6:ae35/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:259 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:30951 (30.2 KiB)  TX bytes:31293 (30.5 KiB)
          Interruption:16 Adresse de base:0x2000

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:H□te
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:10.1.11.1  P-t-P:10.1.11.2  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Parfait ça marche.

2.2) La Politique de sécurité:

Par rapport à la sécurité nous avons proposé d'implémenter IPCop comme pare feu pour bien maîtriser notre réseau et d'implémenter l'antivirus F-secure. Dans toutes les caisses de base.

A. Définition d'IPCop :

IPCop est un projet Open Source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau. Ce système d'exploitation à part entière fonctionne sur une machine dédiée, et utilise très peu de ressources systèmes (un ordinateur PC équipé de 64 Mo de mémoire vive et d'un processeur à 233 MHz suffit). Plus concrètement, IPCop va jouer le rôle d'intermédiaire entre un réseau considéré comme non sûr (Internet) et un réseau que l'on souhaite sécuriser (le réseau local par exemple), tout en fournissant des services permettant la gestion et le suivi de celui-ci.

B. Les interfaces d'IPCop :

La partie Firewall d'IPCop se compose de plusieurs interfaces dont chacune peut être ou non utilisée, à l'exception de l'interface rouge, qui elle, est obligatoire :

- **Rouge**
  Zone du réseau à risque (Internet).

- **Vert**
  Zone du réseau à protéger (réseau local).

- **Bleu**

  Zone spécifique pour les périphériques sans fil. Il n'est possible de faire communiquer l'interface Verte et l'interface Bleu qu'en créant un VPN

- **Orange**

  Zone démilitarisée (DMZ), cette zone est considérée comme publique, elle est accessible de l'extérieur mais ne possède aucun accès sortant (pour des serveurs web par exemple).

Le routage s'effectue de façon automatique entre l'interface d'entrée du trafic (rouge) et les interfaces de sortie (vert, bleu et orange). Il suffit pour cela que chaque machine possède comme passerelle l'adresse IP de la carte d'interface derrière laquelle elle se situe (par exemple 10.255.255.1 comme passerelle car il s'agit de l'adresse IP de l'interface verte).

C. Schéma réseau réalisable avec IPCop :

Voici un exemple plus parlant de schéma réseau réalisable avec IPCop

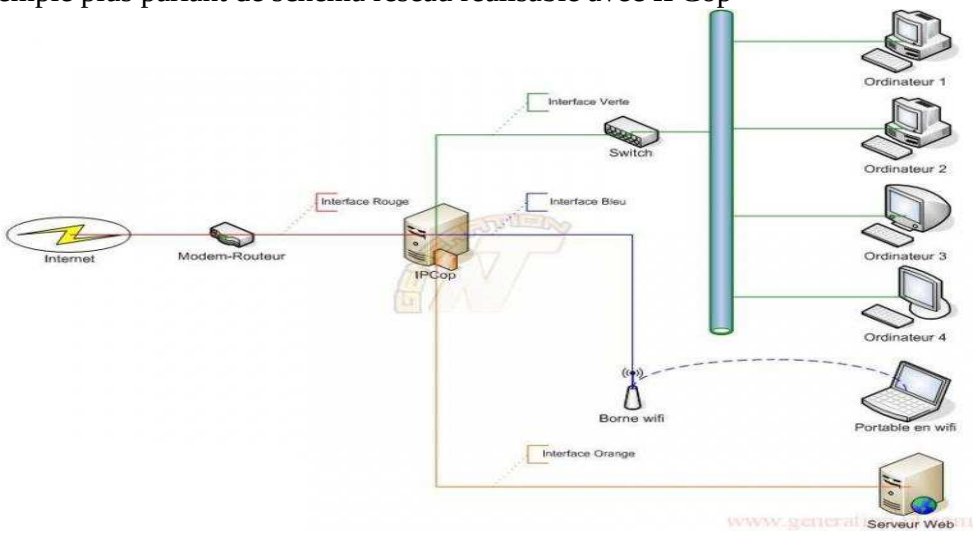


***Figure 1.4.5** : Schéma du réseau réalisable avec IPCop*

Chapitre 4: Planning du déploiement de notre solution :

1) les étapes du projet et leur durée

Les taches	***La durée***
Phase étude de cadrage	15jours
Etudes d'impacts	20 jours
Spécifications fonctionnelles et détaillées	40 jours
Conception des Jeux d'essai pour préparer la recette de la solution	30 jours
Recette d'intégration	90 jours
Simulations de bascule	15 jours
Bascule	2 jours
Post-bascule	20 jours
TOTAL	**232 jours**

Durée prévisionnelle : 11 mois

2) le tableau prévisionnel (Année 2009)

Mois / ***Taches***	**Fev**	**Mars**	**Avril**	**Mai**	**Juin**	**Juill**	**Aout**	**Sep**	**Octo**	**Nov**	**Dec**	**Janv**
Etude de cadrage	--											
Etudes d'impacts	--	--										
Spécifications fonctionnelles détaillées		--	---	---								
Conception des Jeux d'essai pour préparer la recette de la solution					----	---						
Recette d'intégration						-	----	----	----			
Simulations de bascule 1							---					
Simulations de bascule 2									---			
Bascule										-	-	
Post bascule											---	-

Chapitre 5 : Evaluation et le budget financière du nouveau système :

Estimation de l'infrastructure réseau et équipements informatiques :

Désignation	**Prix Unitaire**	**Quantité**	**Total**
Serveur ML 35 G5 N° série 47 00 64-482	3 500 000	1	3 500 000
UC P4 1.6Ghz 256Mo 20Go	90 000	35	3 150 000
Cartes Réseaux	2 500	36	90 000
Pare feu (IpCop)	Free	-	0
Fedora 7	Free	-	0
OpenVPN Windows	Free	-	0
		TOTAL a	**6 740 000 Fcfa**

Type de ligne	**Qté**	**Frais d'accès**	**Total**
Frais accès ligne IP Fixe mono 512k	1	50 000	50 000
Numéris secours régies 512 kbit/s	35	400 002,58	14 000 090,30
		TOTAL b	**14 050 090,30 Fcfa**

TOTAL= TOTAL a+ TOTAL b= (6 740 000 +14 050 090, 30) = 20 790 090, 30 Fcfa

NB :

- la redevance mensuelle de ligne IP fixe mono 512 K est de **57 683** F HTVA
- la redevance mensuelle de linge Numéris secours 512 Kbit/s **634 099** F HTVA

Conclusion :

Arrivé au terme de la rédaction de notre mémoire, nous pouvons dire que l'élaboration de ce travail nous a permis acquérir des connaissances dans les domaines suivants :

- la mise en place d'un VPN sous Linux et Windows;
- les différents éléments actifs servant dans la mise en place d'un système d'interconnexion ;
- les différents protocoles intervenants dans la transmission des données dans le réseau VPN;

En outre, le fait d'avoir pu faire notre études au sein de l'UMECUDEFS nous a permis de pourvoir observer de près certains éléments comme des serveurs tournants sur Linux, des logiciels et des applications open source.

Cette expérience enrichissante d'un point de vue scolaire et professionnel nous a aussi permis de comprendre la réel importance de l'utilisation des VPN dans les entreprises actuelles pour la sécurité, la rapidité, la fiabilité et l'économie dans la transmission de données quand celui est correctement implémenter pour répondre aux mieux aux attentes des actuels utilisateurs de ce genre de services.

En fin Ce mémoire est un outil permettant aux sociétés plus particulièrement à l'UMECUDEFS de mieux appréhender ce saut technologique et de permettre de mettre en place un systèmes d'interconnexion VPN basé sur la solution open source OpenVPN; fonctionnel et offrant plusieurs fonctionnalités.

Au cours de ce travail de recherche au sein de l'UMECUDEFS, nous nous sommes initié au métier d'ingénieur et avons pu comprendre le fonctionnement de la VPN en général et OpenVPN en particulier. Nous avons aussi approfondi nos connaissances en sécurité informatique, Télécommunications et en réseau.

Table des matières

Bibliographie et Webographie

Webographie

www.fedora-fr.org/

www.cisco.com

www.wikipedia.com

www.commentcamarche.com

www.frameip.com

www.openvpn.net/

www.openmaniak.com/fr/openvpn.php

www.ipcop.org/

www.orange.sn

http://ccna.famillecattan.com/

http://www.microsoft.com/france/technet/solutions/RAS/ch8_base.mspx

http://supinfo-projects.com

http://www.supinfo.fr/

www.laboratoire-microsoft.org

Bibliographie

- Configuration Routeur Cisco commandes de base

  Aide mémoire

  Auteur : Benjamin KITTLER 2004 www.kittler.fr/

- ***Construire un VPN sous IP avec Linux***

  Auteur**:** Oleg Kolesnikov, Brian Hatch

Mémoires et les rapports

- **Georges LHUISSIER** Rapport de projet annuel Master Pro RADI-Année : 2007-2008 Université de Caen « ACCES VPN »

Glossaire

A
ADSL : Asymmetric Digital Subscriber Line **ATM**: Asynchronous Transfer Mode **AUI** : Attachment Unit Interface ou interface d'attachement **ARP** : Address resolution protocol (protocole de résolution d'adresse) **AAL** : (ATM Adaptation Layer ou Couche d'adaptation ATM **ASYNC** : C'est le raccourci d'asynchrone. **AH** : (Authentication Header)
B
BGP: Border Gateway Protocol **BISDN**: Broadband Integrated Services Digital Network **BIOS** : Basic Input Output System (système élémentaire d'entrée/sortie)
C
CVC : Circuits Virtuels Commutés **CVP** : Circuits Virtuels Permanent **CSLIP** : Compressed Serial Link Internet Protocol **CSU** : Channel Service Unit **CHAP** : Challenge Handshake Authentication Protocol **CRC** : Cyclic Redundancy Check ou contrôle de redondance cyclique **CIR** : Committed Information Rate **CCS** : Clear Channel Signaling ou Common Channel Signaling **CRL** : (certificate revocation list) **CAST** : (Carlisle Adams et Stafford Tavares)
D
DSL : Digital Subscriber Line **DSU** : Data Service Unit **DDS** : Digital Data Service **DTE** : Data terminal equipment, **DCE** : Data Communication Equipment, soit en français, équipement de communication du circuit de données (ETCD). Exemple d'équipement : le modem. **DLCI** : (Data Link connexion Identifiers) canaux de communication semi-permanents similaires à des trames. **DOD** : département de la Défense des États-Unis (United States Department of Defense, abrégé par DoD ou par DOD) **DNS** : Domain Name System (système de noms de domaine) **DoS** : déni de service ou Denial of Service **DHCP** : Dynamic Host Configuration Protocol **DES** :(Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) **DMZ** : zone démilitarisée (de l'anglais demilitarized zone)
E
EGP : Exterior Gateway Protocol **E-LSR** : Edge Label Switch Router **ESP** : (Encapsulating Security Payload)
F
FDDI : Fiber Distributed Data Interface

FEC : Forward Error Correction **FEC** : forwarding équivalence classes **FTP** : File Transfer Protocol (protocole de transfert de fichiers) **FBI** : Bureau fédéral d'investigation
G
GMT : Greenwich Mean Time **GUID** :(abréviation de l'anglais Globally Unique IDentifier) **GRE** :(Generic Routing Encapsulation) ou Encapsulation Générique de Routage)
H
HDSL : High-speed Digital Subscriber Line **HDLC** : High-Level Data Link Control **HTML** : **Hypertext Markup Language** **HTTP** :HyperText Transfer Protocol, « protocole de transfert hypertexte »
I
IMF : Institut de microfinance **IDSN** : International Dalit Solidarity Network **IETF** : Internet Engineering Task Force **IP** : Internet Protocol **ISO** : Organisation internationale de normalisation **ICMP** : Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. **IGMP** : (Internet Group Management Protocol) est un protocole utilisé pour accéder à un groupe multicast IP **IPX** : Internetwork Packet Exchange **IPSEC** : (Internet Protocol Security)
J
K
L
LAN : Local Area Network **LSR** : Label Switched Router **LIB** : Label Base Information **LSP** : Label Switched Path **L2TP** : (Layer 2 Tunneling Protocol) **L2F** : Layer 2 Forwarding (transfert de couche 2 en français) **LAC** : (L2TP Access Concentrator) **LNS** : (L2tp Network Server) **LDAP** : (Lightweight Directory Access Protocol)
M
MAN : Metropolitan Area Network, réseaux métropolitains. **MPLS** : Multi-Protocol Label Switching. **MAC** **:** (Media Access Control address). **ROM** : Read Only Memory, « mémoire à lecture seule », ou « mémoire morte » **MD5** : Message Digest 5. **MS-CHAP** : (Microsoft Challenge Handshake Authentication Protocol). **MPPE** : (Microsoft Point-to-Point Encryption).

MPPC :(Microsoft Point to Point Compression).
N
NFS : système de fichiers en réseau (Network File System). **NTFS** : New Technology File System **NAT** : Network Address Translation
O
OSI : Open Systems Interconnection, « Interconnexion de systèmes ouverts » **OS** : Operating System en anglais, un système d'exploitation en français ;
P
PVC : Permanent Virtual Circuits **PPP** : Point to Point Protocol **PAP** : Password Authentication Protocol **PSTN** : Public Switched Telephone Network **PKI** : Public Key Infrastructure **PPTP** :(Point-to-point tunneling protocol)
Q
R
RTC : Réseau Téléphonique Commuté **RNIS** : Réseau Numérique à Intégration de Service **RADSL** : Rate Adaptive Digital Subscriber Line **RAID** : Redundant Array of Inexpensive Disks **RSA** : Rivest Shamir Adleman
S
SVC : Switched Virtual Circuits **SLIP** : Serial Line Internet Protocol **SONET** : Synchronous optical networking **SMDS** : Switched Multimegabit Data Service **SDH** : Synchronous digital hierarchy **SMTP** : Simple Mail Transfer Protocol (littéralement « Protocole simple de transfert de courrier »). **SNMP** : Simple Network Management Protocol , protocole simple de gestion de réseau en Français. **SHA-1** : Secure Hash Algorithm) **SSL** : (Secure Sockets Layer), **SPI** : (Security Parameters *Index)* **SA** : (Security Associations) **IKE** : (Internet Key Exchange)
T
TTL : Transistor-Transistor Logic **Telnet** : (TErminal NETwork ou TELecommunication NETwork, ou encore TELetype NETwork) **TCP** : Transmission Control Protocol (littéralement, « protocole de contrôle de transmissions ») **TFTP** : (pour Trivial File Transfert Protocol ou Protocole simplifié de transfert de fichiers) est un protocole simplifié de transfert de fichiers. **TCPA** : Trusted Computing Platform Alliance

TLS : Transport Layer Security
U
UNACOIS : Union Nationale des Commerçants et Industriels du Sénégal **UDP** : User Datagram Protocol (en français protocole de datagramme utilisateur)
V
VPN : Virtual Private Network **VDSL** : Very high bit-rate Digital Subscriber Line **VPI** : Identificateur de Chemin Virtuel **VCI** : Identificateur de Canal Virtuel
W
WAN : Wide Area Network
X
Y
Z

Annexes

Annexes 1 : Mise en œuvre de la politique de la sécurité.

IPTABLES:

Iptables est un outil utilisé pour configurer Netfilter et doit être lancé en que root. Netfilter, quant à lui, est un module du noyau disponible depuis la version du noyau 2.4. Il apporte trois principales fonctionnalités:

- Filtrage de paquets - accepte ou rejette des paquets

- NAT - Change l'adresse IP source ou destination de paquets réseau.

- Modification de paquets - Modifie la structure des paquets

Le but pour nous est d'ouvrir seulement les ports requis et de fermer tous les autres pour limiter des attaques potentielles sur nos systèmes Linux.

La stratégie de sécurité de notre étude de cas est la suivante: Règles de filtrage:

- Ouverture des ports utilisés par OpenVPN pour générer le tunnel entre les deux Linux.
- Ouverture des 80 et 443 ports vers l'extérieur pour laisser les machines locales surfer sur Internet.

- Acceptation de tout le trafic à l'intérieur du tunnel.

- Rejet de tout autre trafic.

Configuration du serveur OpenVPN Linux:

- ANNULATION DES PARAMETRES IPTABLES EXISTANT:

#iptables -F

- STRATEGIES PAR DEFAUT:

Configuration des règles pour rejeter par défaut tout les trafics entrant et sortant et accepter le trafic "Forward" (trafic inter-interface:)

#iptables -P OUTPUT DROP

#iptables -P INPUT DROP
#iptables -P FORWARD ACCEPT

- REGLES OPENVPN:
Autorisation du tunnel OpenVPN:

Exemple d'adresse ip public 213.154.81.15 qui on utilisation

#iptables -A INPUT -i eth0 -p udp -s 0.0.0.0 -d 213.154.81.15 --sport 2001 --dport 2000 -j ACCEPT
#iptables -A OUTPUT -o eth0 -p udp -s 213.154.81.15 -d 0.0.0.0 --sport 2000 --dport 2001 -j ACCEPT

Autosization de tous les trafics à l'intérieur du tunnel:

#iptables -A INPUT -i tap+ -p all -j ACCEPT
#iptables -A OUTPUT -o tap+ -p all -j ACCEPT

- INTERFACE LAN
Tous les trafics de et vers l'interface LAN (eth1) sont acceptés:

#iptables -A INPUT -i eth1 -p all -s 10.1.0.0/16 -j ACCEPT
#iptables -A OUTPUT -o eth1 -p all -d 10.1.0.0/16 -j ACCEPT

- ACCES INTERNET:

Règles de NAT:

Les utilisateurs du réseau local direction doivent être capable de surfer sur Internet impliquant des paramètres de NAT.

Par exemple, quand le poste de travail situé sur le site siége veut accéder une page web sur Internet, son adresse IP source est traduite et prend l'adresse IP WAN de la passerelle. En d'autres termes, 10.1.11.101 est traduit en **213.154.81.15** et vice versa quand les paquets reviennent au poste de travail.

Ce type de NAT est appelé "masquerade".

#iptables -t nat -A POSTROUTING -j MASQUERADE

Autorisation de l'accès Internet:
Les utilisateurs LAN sont autorisés à accéder uniquement à des ressources HTTP ou HTTPS:

#iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -o eth0 -m state --state NEW,ESTABLISHED -j ACCEPT
#iptables -A INPUT -p tcp -m multiport --sports 80,443 -i eth0 -m state --state ESTABLISHED -j ACCEPT

- VERIFICATIONS
Vérifiez la table de routage du Pare-feu:

#iptables -v -L
Chain INPUT (policy DROP 13 packets, 683 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	udp	--	eth0	*	0.0.0.0/0	**213.154.81.15**	udp spt:2001 dpt:2000
4	272	ACCEPT	0	--	tap+	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	0	--	eth0	*	10.1.0.0/16	0.0.0.0/0	
0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443 state ESTABLISHED
4	336	ACCEPT	icmp	--	eth0	*	0.0.0.0	**213.154.81.15**	
0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	**213.154.81.15**	tcp spt:22 state ESTABLISHED
157	10884	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	**213.154.81.15**	tcp dpt:22

Chain FORWARD (policy ACCEPT 5 packets, 217 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination

Chain OUTPUT (policy DROP 339 packets, 110K bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	udp	--	*	eth0	**213.154.81.15**	**213.154.81.15**	udp spt:2000 dpt:2001
		ACCEPT	0	--	*	tap+	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	0	--	*	eth0	0.0.0.0/0	10.1.0.0/16	
0	0	ACCEPT	tcp	--	*	eth0	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
4	336	ACCEPT	icmp	--	*	eth0	**213.154.81.15**	0.0.0.0	
0	0	ACCEPT	tcp	--	*	eth0	**213.154.81.15**	0.0.0.0/0	tcp dpt:22
173	22594	ACCEPT	tcp	--	*	eth0	**213.154.81.15**	0.0.0.0/0	tcp spt:22 state ESTABLISHED

Vérifiez la table NAT:

#iptables -L -t nat

Chain INPUT (policy DROP 13 packets, 683 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination

Chain FORWARD (policy ACCEPT 5 packets, 217 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
108	9273	MASQUERADE	0	- -	any	eth0	anywhere	

Chain OUTPUT (policy DROP 339 packets, 110K bytes)

pkts	bytes	target	prot	opt	in	out	source	destination

OpenVPN Client Linux Configuration:

- ANNULATION DES PARAMETRES IPTABLES EXISTANT:

#iptables -F

- STRATEGIES PAR DEFAUT:

Configuration des règles pour rejeter par défaut tout les trafics entrant et sortant et accepter le trafic "Forward" (trafic inter-interface:)

#iptables -P OUTPUT DROP
#iptables -P INPUT DROP
#iptables -P FORWARD ACCEPT

- REGLES OPENVPN:
Autorisation du tunnel OpenVPN:

#iptables -A INPUT -i eth0 -p udp -s 213.154.80.80**-d 0.0.0.0 --sport 2000 --dport 2001 -j ACCEPT**
#iptables -A OUTPUT -o eth0 -p udp -s 0.0.0.0 -d 213.154.80.80**--sport 2001 --dport 2000 -j ACCEPT**

Autorisation de tous le trafic à l'intérieur du tunnel:

#iptables -A INPUT -i tap+ -p all -j ACCEPT
#iptables -A OUTPUT -o tap+ -p all -j ACCEPT

- INTERFACE LAN
Tous le trafic de et vers l'interface LAN (eth1) est accepté:

#iptables -A INPUT -i eth1 -p all -s 10.12.0.0/16 -j ACCEPT
#iptables -A OUTPUT -o eth1 -p all -d 10.12.0.0/16 -j ACCEPT

- ACCES INTERNET:

Règles de NAT:

Les utilisateurs du réseau local B doivent être capable de surfer sur Internet impliquant des paramètres de NAT.

Par exemple, quand le poste de travail situé sur le site A veux accéder une page web sur Internet, son adresse IP source est traduite et prend l'adresse IP WAN du serveur OpenVPN. En d'autres termes, 10.12.121.0 est traduit en ip public comme (213.154.80.80) et vice versa quand les paquets reviennent au poste de travail.

Ce type de NAT est appelé "masquerade".

#iptables -t nat -A POSTROUTING -j MASQUERADE

Autorisation de l'accès Internet:

Les utilisateurs LAN sont autorisés à accéder uniquement à des ressources HTTP ou HTTPS:

#iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -o eth0 -j ACCEPT
#iptables -A INPUT -p tcp -m multiport --sports 80,443 -i eth0 -m state --state ESTABLISHED -j ACCEPT

.ROUTAGE

Routes réseau

Pour établir le lien entre des machines des LANs du site A et B, les routes suivantes doivent être ajoutées sur les équipements VPN.

Sur le serveur OpenVPN:
Réseau destination 10.12.0.0 masque 255.255.0.0 passerelle 10.12.0.1
Sur le client OpenVPN:
réseau destination 10.1.0.0 masque 255.255.0.0 passerelle 10.1.0.1

Les deux routes sont automatiquement ajoutées avec notre configuration du serveur. En effet, la route du serveur OpenVPN est ajoutée avec le script "route.txt" et la route du client OpenVPN est poussée par le serveur OpenVPN.

- IP forwarding (Redirection IP)

L'IP forwarding est requis pour transférer des paquets entre les interfaces réseau d'un système Linux

#echo "1" > /proc/sys/net/ipv4/ip_forward

La commande ci-dessus va ajouter la valeur "1" dans le fichier /proc/sys/net/ipv4/ip_forward et ainsi activer l'IP forwarding.
Si vous voulez garder l'IP forwarding après un redémarrage:

#echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf

- **. VERIFICATIONS:**

Les clients (11.1.11.100 et 10.12.121.100) devraient être capable de se voir l'un l'autre et accéder à des ressources HTTP et HTTPS sur Internet.

- Test de connectivités LAN à LAN:

Les clients (11.1.11.100 et 10.12.121.100) devraient être capable de se voir l'un l'autre.
Les commandes ping et traceroute peuvent être utilisées à ce propos.
Depuis le client 11.1.11.100qui est une machine Linux:

#ping 10.12.121.100

#traceroute 10.12.121.100

traceroute to 10.12.121.100 *(*10.12.121.100*), 30 hops max, 40 byte packets*
1 11.1.11.100 *(*11.1.11.100*) 0.521 ms 0.848 ms 1.011 ms*

2 10.12.121.1 (10.12.121.1) 0.420 ms 0.472 ms 0505 ms

3 10.12.121.100 *(*10.12.121.100*) 0.538 ms * *

. SCRIPT DE DEMARRAGE

OpenVPN

Le logiciel OpenVPN est configuré pour être lancé automatiquement quand le système démarre.

Pour configurer manuellement OpenVPN pour être lancé automatiquement au démarrage:

#update-rc.d openvpn defaults

Pour prévenir OpenVPN de démarrer automatiquement au démarrage:

#update-rc.d -f openvpn remove

IPtables

Les commandes IPtables ont besoin d'être ajoutée dans un fichier appelé "iptables.sh" qui sera exécuté quand le système Linux démarre Le fichier étant stocké dans le dossier /root Ajoutez une ligne dans le fichier /etc/crontab pour démarrer les commandes IPtables automatiquement à chaque démarrage:

#vim /etc/crontab
@reboot root /root/iptables.sh >> /dev/null

La toute dernière chose à faire est de configurer les permissions du fichier /root/iptables.sh.

L'utilisateur root a les permissions lecture/écriture/exécution. N'importe qui d'autre n'a aucune permission.

#chmod 700 /root/iptables.sh

L'utilisateur root est le propriétaire du fichier /root/iptables.sh.

#chown root /root/iptables.sh

Annexes 2: Factures Proforma